OTONIEL NOGUEIRA DA SILVA

A cota de Andersen-Geil para distância mínima de códigos e aplicações

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2013

OTONIEL NOGUEIRA DA SILVA

A cota de Andersen-Geil para distância mínima de códigos e aplicações

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para obtenção do título de **MESTRE EM MATEMÁTICA.**

Área de Concentração: Matemática.
Linha de Pesquisa: Geometria Algébrica.

Orientador: Prof. Dr. Cícero Fernandes de Carvalho.

UBERLÂNDIA - MG
2013

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da UFU , MG, Brasil

S586c 2012

Silva, Otoniel Nogueira da, 1988-
A cota de Andersen-Geil para distância mínima de códigos e aplicações / Otoniel Nogueira da Silva. - 2013.
43 p. : il.

Orientador: Cícero Fernandes de Carvalho.

Dissertação (mestrado) – Universidade Federal de Uberlândia, Programa de Pós-Graduação em Matemática.
Inclui bibliografia.

1. Matemática - Teses. 2. Bases de Gröbner - Teses. 2. Códigos de Goppa - Teses. 3. Equações diferenciais ordinárias - Teses. I. Carvalho, Cícero Fernandes de. II. Universidade Federal de Uberlândia. Programa de Pós-Graduação em Matemática. III.Título.

CDU: 51

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 152
Campus Santa Mônica, Uberlândia - MG, CEP 38400-902

ALUNO: Otoniel Nogueira da Silva.

NÚMERO DE MATRÍCULA: 11112MAT007.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Geometria Algébrica.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: A cota de Andersen-Geil para distância mínima de códigos e aplicações.

ORIENTADOR: Prof. Dr. Cícero Fernandes de Carvalho.

Esta dissertação foi **APROVADA** em reunião pública realizada na Sala Multiuso da Faculdade de Matemática, Bloco 1F, Campus Santa Mônica, em 25 de fevereiro de 2013, às 10h00min, pela seguinte Banca Examinadora:

NOME	ASSINATURA
Prof. Dr. Cícero Fernandes de Carvalho UFU - Universidade Federal de Uberlândia	
Prof. Dr. Paulo Roberto Brumatti UNICAMP - Universidade Estadual de Campinas	
Prof. Dr. Victor Gonzalo Lopez Neumann UFU - Universidade Federal de Uberlândia	

Uberlândia-MG, 25 de fevereiro de 2013.

Dedicatória

Dedico primeiramente a Deus, pois sem Ele eu nunca teria chegado até este ponto de minha vida. Dedico aos meus pais Oracildo e Marta, e dedico também a minha esposa Núbia que em momentos de dificuldade sempre me deu forças para continuar, além de muito carinho e amor. Dedico ao meu tio Horácio e minha avó Geralda que sempre me apoiaram em meus estudos. E, aos meus familiares e amigos, que sempre acreditaram em mim e nunca duvidaram da minha capacidade. Obrigado a todos, Deus abençõe vocês.

Agradecimentos

Agradeço primeiramente a Deus. Agradeço a agência CAPES pelo fornecimento da bolsa de pesquisa ao longo da Pós-Graduação; ao meu orientador Cícero Fernandes de Carvalho pelos ensinamentos e conselhos dados e aos professores Paulo Roberto Brumatti e Victor Gonzalo Lopez Neumann por terem aceito o convite para fazerem parte da minha banca.

SILVA, O. N. *A cota de Andersen-Geil para distância mínima de códigos e aplicações.* 2013. 43 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Neste trabalho, estudamos a teoria dos domínios de ordem com aplicações nos códigos lineares, em particular; nos códigos de Goppa de um ponto. Também estudamos algumas teorias que nos serviram como base teórica tais como: a teoria de corpos de funções algébricas, a teoria das bases de Gröbner e uma breve introdução sobre geometria algébrica. Este trabalho tem por objetivo apresentar uma cota para a distância mínima de um código linear dada por Andersen-Geil na referência [1], além de apresentar uma maneira de construir códigos usando a teoria dos domínios de ordem. Para finalizar, trabalhamos com alguns exemplos de códigos de comprimentos maiores, neste caso; usamos a teoria das bases de Gröbner como ferramenta.

Palavras-chave: Bases de Gröbner; Códigos de Avaliação; Códigos de Goppa; Distância mínima; Domínio de Ordem; Pegada.

SILVA, O. N. *The Andersen-Geil bound for minimum distance of codes and applications*. 2013. 43 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

In this work, we study the theory of order domains with applications in linear codes, in particular; in one-point Goppa codes. We also studied some theories that served as the basis theoretical such as the theory of algebraic function fields, the theory of Gröbner bases and a brief introduction about algebraic geometry. This work aims to introduce a bound for the minimum distance of a linear code givem by Andersen-Geil in reference [1], and present a way to construct codes using the theory of order domains. Finally, we work some examples of codes with longer lengths, in this case; we use the theory of Gröbner bases as a tool.

Keywords:Evaluation Codes; Footprint; Goppa codes; Gröbner bases; Minimum distance; Order Domain.

Sumário

Introdução

Este trabalho trata de códigos corretores de erros, em particular, de cotas para distância mínima de um código. Os códigos corretores de erros participam da vida moderna de inúmeras formas como, por exemplo, nas comunicações via satélite, na telefonia celular e na comunicação entre computadores. Um dos fundadores da teoria dos códigos corretores de erros foi o matemático americano *Claude Elwood Shannon*. Em 1948, Shannon publicou um importante artigo científico (que é a referência [12]) que tinha como título: *"A Mathematical Theory of Communication"*, enfocando o problema de qual é a melhor forma para codificar uma informação que um emissor queira transmitir para um receptor. Inicialmente, os maiores interessados na teoria dos códigos foram os matemáticos que a desenvolveram consideravelmente nas décadas de 50 e 60. A partir da década de 70, com as pesquisas espaciais e a grande popularização dos computadores, essa teoria começou a interessar também aos engenheiros, e desde então tem sido muito estudada.

Este trabalho está dividido em quatro capítulos. No primeiro capítulo, veremos apenas alguns conceitos e resultados básicos da teoria de códigos corretores de erros tais como: distância mínima, dimensão e comprimento de um código. Apresentamos também a cota de Singleton que é um resultado clássico da teoria de códigos, e apresentamos os códigos de Reed-Solomon para introduzirmos a primeira seção do próximo capítulo. No segundo capítulo, apresentamos um exemplo motivador e obtemos nesse exemplo a distância mínima dos códigos de Reed-Solomon de uma forma não tradicional, em seguida apresentamos o método de Andersen-Geil para obter uma cota para a distância mínima de códigos. Ainda no segundo capítulo, trabalhamos com pesos generalizados de Hamming, apresentamos a cota de Feng-Rao para os pesos generalizados de Hamming e mostramos que a cota de Shibuya e Sakaniwa pode ser vista como uma consequência da cota de Andersen-Geil.

O método apresentado no capítulo 2 não é muito prático se estivermos tratando de códigos no contexto geral, por esse motivo na construção de códigos precisamos de uma certa estrutura algébrica para aplicarmos o método de Andersen-Geil, assim no capítulo 3 introduzimos o conceito de domínios de ordem e estrutura de ordem, e construimos os códigos da teoria dos domínios de ordem. Ainda no capítulo 3, mostramos que todo código de Goppa de um ponto pode ser visto como sendo um código da teoria dos domínios de ordem.

Para códigos de grandes comprimentos precisamos usar um método mais sofisticado, assim no capítulo 4 trabalhamos com as bases de Gröbner em conjunto com o método de Andersen-Geil. Para finalizar, colocamos alguns exemplos que ilustram como o método de Andersen-Geil funciona.

Otoniel Nogueira da Silva
Uberlândia-MG, 25 de fevereiro de 2013.

Capítulo 1

Preliminares

1.1 Códigos Lineares

Vamos introduzir algumas noções básicas da teoria de códigos, o leitor menos familiarizado com estes conceitos pode consultar qualquer livro sobre códigos corretores de erros, uma sugestão é a referência [11]. Seja $\mathbb{F}_q$ um corpo finito com q elementos. Consideramos o espaço vetorial $\mathbb{F}_q^n$ de dimensão n, cujo os elementos são n-uplas $a = (a_1, \cdots, a_n)$ com $a_i \in \mathbb{F}_q$.

Definição 1.1.1 *Para $a = (a_1, \cdots, a_n)$ e $b = (b_1, \cdots, b_n) \in \mathbb{F}_q^n$ definimos*

$$d(a, b) := \sharp(\{i;\ a_i \neq b_i\}).$$

Esta função d é chamada de distância de Hamming sobre $\mathbb{F}_q^n$. O peso de um elemento $a \in \mathbb{F}_q^n$ é definido como

$$w(a) := d(a, 0) = \sharp(\{i; a_i \neq 0\}).$$

A distância de Hamming é uma métrica sobre $\mathbb{F}_q^n$, em particular a desigualdade triangular ocorre.

Definição 1.1.2 *Um código C (sobre o alfabeto $\mathbb{F}_q^n$) é um subespaço linear de $\mathbb{F}_q^n$; os elementos de C são chamados de palavras. Chamamos de n o comprimento de C e $dim(C)$ (como $\mathbb{F}_q^n$-espaço vetorial) a dimensão de C. Um código $[n, k]$ é um código de comprimento n e dimensão k. A distância mínima $d(C)$ de um código $C \neq 0$ é definida como*

$$d(C) := \ min\{d(a, b) \mid a, b \in C \text{ e } a \neq b\} = min\{w(c) \mid c \neq 0 \in C\}.$$

Um [n,k,d] é um código de comprimento n, dimensão k e distância mínima d.

Uma maneira simples de descrever um código C explicitamente é por meio de uma base de C (como $\mathbb{F}_q$-espaço vetorial).

Definição 1.1.3 *Seja C um $[n, k]$ código sobre $\mathbb{F}_q$. Uma matriz geradora de C é uma matriz $k \times n$ cujas as linhas formam uma base para C.*

Definição 1.1.4 *O produto interno canônico sobre $\mathbb{F}_q^n$ é definido por*

$$\langle a, b\rangle := \sum_{i=1}^{n} a_i b_i,$$

para $a = (a_1, \cdots, a_n)$ e $b = (b_1, \cdots, b_n) \in \mathbb{F}_q^n$.

Definição 1.1.5 *Se $C \subseteq \mathbb{F}_q^n$ é um código, então*

$$C^{\perp} := \{u \in \mathbb{F}_q^n \mid \langle u, c\rangle = 0 \text{ para todo } c \in C\}$$

é chamado de dual de C.

Observação 1.1.6 *Sabemos da álgebra linear que o dual de um $[n,k]$ código é um $[n, n-k]$ código, e $(C^{\perp})^{\perp} = C$.*

Definição 1.1.7 *Uma matriz geradora H de $C^{\perp}$ é chamada de matriz checagem de paridade de C.*

Observação 1.1.8 *Claramente uma matriz checagem de paridade H de um $[n,k]$ código é uma matriz $(n-k) \times (n)$, e ainda temos que*

$$C = \{u \in \mathbb{F}_q^n \mid H.u^t = 0\}$$

(onde u^t denota a matriz(vetor) transposta de u). Logo, uma matriz checagem de paridade "checa"quando um vetor $u \in \mathbb{F}_q^n$ é uma palavra do código ou não.

Um dos problemas clássicos da teoria dos códigos corretores de erros é construir (sobre um alfabeto $\mathbb{F}_q$ fixado) um código cuja a dimensão e a distância mínima sejam grandes em comparação com seu comprimento. Contudo, existem algumas restrições. Falando a grosso modo, se a dimensão do código é grande (com relação ao seu comprimento), então a sua distância mínima é pequena, e vice-versa. A próxima proposição mostrará este fato.

Proposição 1.1.9 ***(A cota de Singleton).*** *Para um $[n,k,d]$ código C o seguinte acontece:*

$$k + d \leq n + 1$$

Demonstração. Uma prova desta proposição poderá ser encontrada no capítulo 2 da referência [5]. ■

1.2 Códigos de Reed-Solomon

Como uma motivação para o próximo capítulo, iremos apresentar agora os códigos de Reed-Solomon sobre $\mathbb{F}_q$. Esta importante classe de códigos é bem conhecida na teoria dos códigos corretores de erros há um bom tempo. Vamos então à construção desses códigos:

Seja $n = q-1$ e seja $\beta \in \mathbb{F}_q$ um elemento primitivo do grupo multiplicativo $\mathbb{F}_q^* = \{\beta, \beta^2, \cdots, \beta^n = 1\}$. Para um inteiro k, com $1 \leq k \leq n$, consideramos o espaço vetorial de dimensão k:

$$\mathcal{L}_k := \{f \in \mathbb{F}_q[X] \mid grau(f) \leq k-1\}$$

e a aplicação de avaliação $ev : \mathcal{L}_k \to \mathbb{F}_q^n$ dada por:

$$ev(f) := (f(\beta), f(\beta^2), \cdots, f(\beta^n)) \in \mathbb{F}_q^n.$$

Obviamente esta aplicação é $\mathbb{F}_q$-linear, e ela é injetora pois um polinômio não nulo $f \in \mathbb{F}_q[X]$ de grau menor que n tem no máximo n zeros. Portanto,

$$C_k := \{(f(\beta), f(\beta^2), \cdots, f(\beta^n)) \mid f \in \mathcal{L}_k\}$$

é um $[n, k]$ código sobre $\mathbb{F}_q$; e ele é chamado de **código de Reed-Solomon**.

O peso de uma palavra do código $0 \neq c = ev(f) \in C_k$ é dado por:

$$\begin{aligned} w(c) &= n - \sharp(\{i \in \{1, \cdots, n\}; f(\beta^i) = 0\}) \\ &\geq n - grau(f) \geq n - (k-1). \end{aligned}$$

Logo, a distância mínima d de C_k satisfaz a inequação $d \geq n+1-k$. Por outro lado, $d \leq n+1-k$ pela cota de Singleton, assim $d = n + 1 - k$.

Capítulo 2

A cota de Andersen-Geil

2.1 Um exemplo motivador

Nesta seção obtemos a conhecida distância mínima dos códigos de Reed-Solomon de uma forma não tradicional, diferente daquela que fizemos no capítulo 1. O seguinte exemplo nos ajudará a ter uma noção do método usado por Andersen-Geil para encontrar uma cota para a distância mínima de um código. Usaremos também este mesmo exemplo para introduzir e motivar a próxima seção. O texto apresentado neste e nos demais capítulos tem como principal referência um artigo de Henning E. Andersen e Olav Geil que é a nossa referência [1].

Exemplo 2.1.1 *Sejam $P_1, P_2, \cdots, P_q$ os elementos de um corpo $\mathbb{F}_q$. Defina $n := q$ e considere a aplicação de avaliação $ev : \mathbb{F}_q[X] \longrightarrow \mathbb{F}_q^n$ dada por:*

$$ev(F) := (F(P_1), \cdots, F(P_n))$$

É fácil ver que ev é uma aplicação $\mathbb{F}_q$-linear.

O conjunto:

$$B = \{b_1 = ev(1), b_2 = ev(X), \cdots, b_n = ev(X^{n-1})\}$$

é uma base para $\mathbb{F}_q^n$ como um espaço vetorial sobre $\mathbb{F}_q$.

De fato, considere a combinação linear nula abaixo:

$$\lambda_1 ev(1) + \lambda_2 ev(X) + \cdots + \lambda_n ev(X^{n-1}) = 0$$

Definindo $F(X) := \lambda_1 + \lambda_2 X + \cdots + \lambda_n X^{n-1}$ e como ev é linear, então:

$$\lambda_1 ev(1) + \lambda_2 ev(X) + \cdots + \lambda_n ev(X^{n-1}) = 0 \iff ev(\lambda_1 + \lambda_2 X + \cdots + \lambda_n X^{n-1}) = 0 \iff$$
$$ev(F(X)) = 0 \iff (F(P_1), \cdots, F(P_n)) = (0, \cdots, 0)$$

Mas $grau(F) < n$, logo F tem no máximo $n-1$ raízes distintas em $\mathbb{F}_q$. Logo, como $P_1, \cdots, P_n$ são distintos segue que os elementos $b_1, \cdots, b_n$ são linearmente independentes. Como $dim(\mathbb{F}_q^n) = n$, segue que B é uma base para $\mathbb{F}_q^n$.

Para $k = 1, \cdots, n$, o código de Reed-Solomon é dado por:

$$C_k := \ span_{\mathbb{F}_q}\{b_i \mid i = 1, \cdots, k\}$$

Agora, vamos obter a cota $d(C_k) \geq n - k + 1$ de uma maneira não tradicional.

Considere uma palavra do código $c = (c_1, \cdots, c_n) \in C_k$, digamos:

$$c = \sum_{t=1}^{i} \alpha_t b_t, \text{ com } \alpha_1, \cdots, \alpha_i \in \mathbb{F}_q, \ \alpha_i \neq 0 \ e \ i \leq k.$$

Observe que:

$$c = \sum_{t=1}^{i} \alpha_t b_t = \sum_{t=1}^{i} \alpha_t ev(X^{t-1}) = ev\left(\sum_{t=1}^{i} \alpha_t X^{t-1}\right)$$

Para estimar o peso de Hamming de c, faremos uso do seguinte produto em $\mathbb{F}_q^n$:
Sejam $h = (h_1, \cdots, h_n)$, $f = (f_1, \cdots, f_n) \in \mathbb{F}_q^n$, definimos o ***produto de Hadamard*** *de h e f como:*

$$h * f = (h_1 f_1, \cdots, h_n f_n)$$

Agora, observe que:

$$c * b_1 = ev\left(\sum_{t=1}^{i} \alpha_t X^{t-1}\right) \in C_i \backslash C_{i-1}$$

Da mesma forma, temos:

$$c * b_2 = ev\left(\sum_{t=1}^{i} \alpha_t X^{t-1}\right) * ev(X) = ev\left(\sum_{t=1}^{i} \alpha_t X^{t}\right) \in C_{i+1} \setminus C_i$$

$$c * b_3 = ev\left(\sum_{t=1}^{i} \alpha_t X^{t-1}\right) * ev(X^2) = ev\left(\sum_{t=1}^{i} \alpha_t X^{t+1}\right) \in C_{i+2} \setminus C_{i+1}$$

$$\vdots \qquad \vdots \tag{2.1}$$

$$c * b_{n-i+1} = ev\left(\sum_{t=1}^{i} \alpha_t X^{t-1}\right) * ev(X^{n-i}) = ev\left(\sum_{t=1}^{i} \alpha_t X^{n-i+t-1}\right) \in C_n \setminus C_{n-1}$$

Consequentemente, os vetores $c * b_1, c * b_2, \cdots, c * b_{n-i+1}$ são linearmente independentes, e portanto:

$$span_{\mathbb{F}_q}\{c * b_1, c * b_2, \cdots, c * b_{n-i+1}\} \tag{2.2}$$

é um espaço de dimensão $n - i + 1$.

Agora denote por $e_1 := (1, 0, \cdots, 0), e_2 := (0, 1, 0, \cdots, 0), \cdots, e_n := (0, \cdots, 0, 1)$ e seja l o peso de Hamming de c, e digamos que $Supp(c) = \{i_1, i_2, \cdots, i_l\}$, onde $Supp(c)$ é o conjunto $\{i \mid c_i \neq 0\}$. Então:

$$span_{\mathbb{F}_q}\{c * d \mid d \in \mathbb{F}_q^n\} = span_{\mathbb{F}_q}\{e_{i_1}, \cdots, e_{i_l}\} \tag{2.3}$$

De fato, seja $d = (d_1, \cdots, d_n) \in \mathbb{F}_q^n$ e denote $c = (\alpha_1, \cdots, \alpha_n)$, onde $\alpha_{i_1}, \alpha_{i_2}, \cdots, \alpha_{i_l} \neq 0$ e $\alpha_j = 0$, $\forall j \neq i_1, i_2, \cdots, i_l$. Assim:

$$c * d = (\alpha_1 d_1, \cdots, \alpha_n d_n) = (\alpha_1 d_1)e_1 + \cdots + (\alpha_n d_n)e_n = (\alpha_{i_1} d_{i_1})e_{i_1} + \cdots + (\alpha_{i_l} d_{i_l})e_{i_l} \in span_{\mathbb{F}_q}\{e_{i_1}, \cdots, e_{i_l}\}$$

Logo, toda combinação linear de elementos de $\{c * d \mid d \in \mathbb{F}_q^n\}$ *está em* $span_{\mathbb{F}_q}\{e_{i_1}, \cdots, e_{i_l}\}$*, e logo temos:*

$$span_{\mathbb{F}_q}\{c * d \mid d \in \mathbb{F}_q^n\} \subseteq span_{\mathbb{F}_q}\{e_{i_1}, \cdots, e_{i_l}\} \tag{2.4}$$

Por outro lado, temos que $\mathbb{F}_q$ *é corpo e que* $\alpha_{i_1}, \cdots, \alpha_{i_l} \neq 0$*, logo para cada* $s = 1, \cdots, l$ *existe* $\alpha_{i_s}^{-1}$.
Logo, $c * ((\alpha_{i_s})^{-1} e_{i_s}) = (\alpha_1, \cdots, \alpha_n) * (0, 0, \cdots, \alpha_{i_s}^{-1}, 0, \cdots, 0) = (0, 0, \cdots, 1, 0, \cdots, 0) = e_{i_s} \in span_{\mathbb{F}_q}\{c * d \mid d \in \mathbb{F}_q^n\}$*, para* $\forall s = 1, \cdots, l$*. Assim, dim* $(span_{\mathbb{F}_q}\{c * d \mid d \in \mathbb{F}_q^n\}) \geq l$ *mas por (2.4), temos que:*

$$dim\ (span_{\mathbb{F}_q}\{c * d \mid d \in \mathbb{F}_q^n\}) \leq dim\ (span_{\mathbb{F}_q}\{e_{i_1}, \cdots, e_{i_l}\}) = l$$

Logo, segue o que queríamos provar.

É claro que o espaço de dimensão $n - i + 1$ *em (2.2) está contido no espaço de dimensão* l *em (2.3) e portanto* $w_H(c) = l \geq n - i + 1$.
Assim, como $d(C_k) = min\ \{w_H(c) \mid 0 \neq c \in C_k\}$*, temos que:*

$$d(C_k) \geq min\{n - i + 1 \mid i = 1, \cdots, k\} = n - k + 1$$

Mas pela cota de Singleton, temos o resultado usual para os códigos de Reed-Solomon:

$$d(C_k) = n - k + 1$$

Observação 2.1.2 *No exemplo anterior usamos fortemente a estrutura algébrica do anel de polinômios* $\mathbb{F}_q[X]$*. Sem isto, deveria ser bastante difícil concluirmos as inclusões cruciais em (2.1).*

Portanto, quando olhamos para as classes de códigos para os quais o método anterior pode ser aplicado de uma maneira praticável, deveríamos procurar por códigos definidos sobre algumas estruturas algébricas. Apesar disso, continuamos a descrição da cota de Andersen-Geil considerando que ela se aplica no caso geral de qualquer código linear. Neste contexto, o método de Andersen-Geil realmente não é muito praticável.

Contudo, mas a frente no texto, veremos como a cota de Andersen-Geil se aplica muito naturalmente no caso dos códigos vindos da teoria de domínios ordem. Neste contexto, a cota será tão praticável quanto a cota de Feng-Rao, que discutiremos em uma seção posterior.

2.2 A cota de Andersen-Geil para a distância mínima

Esta seção contém uma descrição do método de Andersen-Geil no contexto geral dos códigos lineares. O método tem como objetivo não somente encontrar uma cota para a distância mínima, mas também encontrar uma cota para todos os pesos generalizados de Hamming. Falaremos dos pesos generalizados de Hamming na próxima seção. Usaremos o exemplo motivador da seção anterior como uma diretriz.

Considere a seguinte definição de um código linear:

Definição 2.2.1 *Seja $B = \{b_1, \cdots, b_n\}$ uma base para $\mathbb{F}_q^n$ e seja $G \subseteq B$. Definimos o $\#G-$código dimensional $C(B,G)$ por $C(B,G) := span_{\mathbb{F}_q}\{b \mid b \in G\}$. O código dual (de dimensão $n - \#G$) será denotado por $C^{\perp}(B,G)$.*

Usaremos o seguinte conjunto de espaços:

Definição 2.2.2 *Seja $L_{-1} := \emptyset, L_0 := \{0\}$ e $L_l := span_{\mathbb{F}_q}\{b_1, \cdots, b_l\}$ para $l = 1, \cdots, n$.*

É claro que temos uma cadeia de espaços:

$$\{0\} = L_0 \subsetneqq L_1 \subsetneqq \cdots \subsetneqq L_{n-1} \subsetneqq L_n = \mathbb{F}_q^n$$

Consequentemente, podemos definir uma função, apresentada a seguir.

Definição 2.2.3 *Definimos $\overline{\rho} : \mathbb{F}_q^n \longrightarrow \{0, 1, \cdots, n\}$ por $\overline{\rho}(v) = l$ se $v \in L_l \backslash L_{l-1}$.*

Relembre do exemplo motivador que dado uma palavra código $c \in C(B,G)$, gostaríamos de encontrar tantos diferentes números s quantos possíveis tais que existe um elemento b_j com $c * b_j \in L_s \setminus L_{s-1}$. Isto irá permitir darmos uma boa estimativa para o peso de c. Expressando na linguagem da função $\overline{\rho}$, olhamos para os valores s tais que um b_j existe com $\overline{\rho}(c * b_j) = s$.

Em geral, não é uma tarefa fácil encontrar $\overline{\rho}(c * b_j)$. Isto é o motivo para definirmos agora o conceito de pares bem comportados.

Definição 2.2.4 *Seja $I_n := \{1, 2, \cdots, n\}$. Um par ordenado $(i,j) \in I_n^2$ é dito ser bem comportado (**WB**) se $\overline{\rho}(b_u * b_v) < \overline{\rho}(b_i * b_j)$ para todo u e v com $1 \leq u \leq i$, $1 \leq v \leq j$ e $(u,v) \neq (i,j)$. Um pouco menos restritivo, um par ordenado $(i,j) \in I^2$ é dito ser fracamente bem comportado (**WWB**) se $\overline{\rho}(b_u * b_j) < \overline{\rho}(b_i * b_j)$ para $u < i$ e $\overline{\rho}(b_i * b_v) < \overline{\rho}(b_i * b_j)$ para $v < j$.*

É claro que se $(i,j) \in I_n^2$ é WB, então (i,j) também é WWB. Existe um outra formulação "mais fraca"da definição acima, onde dizemos que um par $(i,j) \in I_n^2$ é fracamente bem comportado por apenas um lado (**OWB**) se $\overline{\rho}(b_u * b_j) < \overline{\rho}(b_i * b_j)$ para $u < i$. No enunciado do teorema da cota de Andersen-Geil que ainda veremos, pode-se trocar a hipótese de (i,j) ser WWB por OWB, porém vamos manter a hipótese de (i,j) ser WWB na cota de Andersen-Geil por causa dos demais resultados que iremos ver.

Exemplo 2.2.5 *Seja $B = \{b_1, b_2\}$ uma base para $\mathbb{F}_5^2$ com $b_1 = (1,2)$ e $b_2 = (3,4)$. É fácil ver que o par $(1,1)$ é o único par WB(e também o único par WWB).*

Observação 2.2.6 *Considere uma palavra do código,*

$$c = \sum_{t=1}^{v} \alpha_t b_{i_t} \text{ com } i_1 < \cdots < i_v \text{ e } \alpha_v \neq 0$$

*Se (i_v, j) é **WWB** então por definição temos que:*

$$\overline{\rho}(b_{i_t} * b_j) < \overline{\rho}(b_{i_v} * b_j) \text{ para } t = 1, 2, \cdots, v-1$$

e portanto podemos concluir que:

$$\overline{\rho}(c * b_j) = \overline{\rho}\left(\left(\sum_{t=1}^{v} \alpha_t b_{i_t}\right) * b_j\right) = \overline{\rho}((\alpha_1 b_{i_1} + \alpha_2 b_{i_2} + \cdots + \alpha_v b_{i_v}) * b_j) =$$

$$\overline{\rho}(\alpha_1(b_{i_1} * b_j) + \cdots + \alpha_v(b_{i_v} * b_j)) = \overline{\rho}\left(\sum_{t=1}^{v} \alpha_t (b_{i_t} * b_j)\right) = \overline{\rho}(b_{i_v} * b_j)$$

Então, para estimar o número de $s's$ tais que existe um elemento b_j da base com $\overline{\rho}(c*b_j) = s$, podemos simplesmente calcular (ou contar) o tamanho do seguinte conjunto (aqui i deve ser trocado por i_v):

Definição 2.2.7

$$\Lambda_i := \{\ l \in I_n \ \mid\ \overline{\rho}(b_i * b_j) = l \text{ para algum } b_j \text{ com } (i,j)\ WWB\ \}$$

Observação 2.2.8 *Se darmos dois diferentes números j_1 e j_2 tais que ambos os pares (i, j_1) e (i, j_2) são WWB, então:*

$$\overline{\rho}(b_i * b_v) < \overline{\rho}(b_i * b_{j_1}) \text{ para } \forall v < j_1 \text{ e}$$

$$\overline{\rho}(b_i * b_v) < \overline{\rho}(b_i * b_{j_2}) \text{ para } \forall v < j_2$$

Suponha sem perda de generalidade que $j_1 < j_2$, logo $\overline{\rho}(b_i * b_{j_1}) < \overline{\rho}(b_i * b_{j_2})$, e portanto:

$$\overline{\rho}(b_i * b_{j_1}) \neq \overline{\rho}(b_i * b_{j_2})$$

Consequentemente, para um número fixo i, contar o tamanho do conjunto Λ_i é o mesmo que contar o número de pares (i, j), $j \in I_n$ que são WWB.

Agora, estamos em condições de enunciar a cota de Andersen-Geil para a distância mínima de um código linear.

Teorema 2.2.9 ***(A cota de Andersen-Geil)*** *A distância mínima de $C(B, G)$ satisfaz:*

$$d(C(B,G)) \geq \ min\ \{\ \#\Lambda_i \mid b_i \in G\ \}$$

Demonstração. Seja $c \in C(B,G)\backslash\{0\}$, então c é da forma:

$$c = \sum_{t=1}^{v} \alpha_t b_{i_t} \text{ com } i_1 < \cdots < i_v \text{ e } \alpha_v \neq 0$$

com i_t satisfazendo $b_{i_t} \in G$, para todo $t = 1, \cdots, v$.

Agora, considere o conjunto Λ_{i_v}, e suponha que Λ_{i_v} seja não vazio, caso contrário $\#\Lambda_{i_v} = 0$ e como $d(C(B,G)) \geq 1$, teríamos que:

$$d(C(B,G)) \geq 0 = \Lambda_{i_v} = min\ \{\ \#\Lambda_i \mid b_i \in G\ \}$$

Supondo que Λ_{i_v} não seja vazio, logo existem $1 \leq l_1 < \cdots < l_{\#\Lambda_{i_v}} \leq n$ e os índices correspondentes $j_1, \cdots, j_{\#\Lambda_{i_v}} \in I_n$ tais que:

$$\overline{\rho}(b_{i_v} * b_{j_1}) = l_1, \text{ com } (i_v, j_1) \text{ WWB}$$

$$\overline{\rho}(b_{i_v} * b_{j_2}) = l_2, \text{ com } (i_v, j_2) \text{ WWB}$$

$$\vdots \qquad\qquad \vdots$$

$$\overline{\rho}(b_{i_v} * b_{j_{\#\Lambda_{i_v}}}) = l_{\#\Lambda_{i_v}}, \text{ com } (i_v, j_{\#\Lambda_{i_v}}) \text{ WWB}$$

Mas pela observação 2.2.6 temos que $\overline{\rho}(c * b_{j_s}) = \overline{\rho}(b_{i_v} * b_{j_s})$, para todo $s = 1, \cdots, \#\Lambda_{i_v}$.

E assim:

$$c * b_{j_1} \in L_{l_1} \setminus L_{l_1 - 1}$$

$$\vdots \qquad\qquad \vdots$$

$$c * b_{j_{\#\Lambda_{i_v}}} \in L_{l_{\#\Lambda_{i_v}}} \setminus L_{l_{\#\Lambda_{i_v}} - 1}$$

Consequentemente, $c * b_{j_1}, \cdots, c * b_{j_{\#\Lambda_{i_v}}}$ são linearmente independentes, e logo o espaço:

$$span_{\mathbb{F}_q}\{c * b_{j_1}, \cdots, c * b_{j_{\#\Lambda_{i_v}}}\} \tag{2.5}$$

tem dimensão $\#\Lambda_{i_v}$. Como no exemplo motivador, o espaço:

$$span_{\mathbb{F}_q}\{\ c * d\ \mid\ d \in \mathbb{F}_q^n\ \} \tag{2.6}$$

tem dimensão igual ao peso de Hamming de c. E como o espaço em (2.5) está contido no espaço em (2.6) concluímos que:

$$w_H(c) \geq \#\Lambda_{i_v}$$

Mas então, é claro que também temos $w_H(c) \geq min\ \{\ \#\Lambda_i \mid b_i \in G\ \}$, e logo:

$$d(C(B, G)) \geq\ min\ \{\ \#\Lambda_i \mid b_i \in G\ \}$$

como queríamos demonstrar. ■

2.3 Uma cota para os pesos Generalizados de Hamming

Veremos nesta seção que o teorema 2.2.9 pode ser extendido com o objetivo de achar uma cota não somente para a distância mínima, mas também para todos os pesos generalizados de Hamming.

O teorema 2.2.9 também pode algumas vezes ser melhorado levemente. A pequena melhoria será importante quando em uma seção posterior compararmos a cota de Andersen-Geil com a cota dada por Shibuya e Sakaniwa.

Antes de dar a versão extendida do teorema 2.2.9, vamos lembrar ao leitor a definição dos pesos generalizados de Hamming.

Definição 2.3.1 *(a) O suporte de um conjunto S, com $S \subseteq \mathbb{F}_q^n$ é definido por:*

$$Supp(S) := \{\ i \mid c_i \neq 0 \text{ para algum } c = (c_1, \cdots, c_n) \in S\ \}$$

(b) O t-ésimo peso generalizado de Hamming de um código C é definido por:

$$d_t(C) := min\{\ \#Supp(S) \mid S \text{ é um subcódigo de } C \text{ de dimensão } t\}$$

Para enunciarmos a extensão do teorema 2.2.9, precisaremos da seguinte definição:

Definição 2.3.2 *Para* $\{i_1, \cdots, i_t\} \subseteq I_n$ *definimos*

$$\overline{\sigma}(i_1, \cdots, i_t) := \#\left(\left(\bigcup_{s=1}^{t} \Lambda_{i_s}\right) \cup \{i_1, \cdots, i_t\}\right)$$

Em particular, $\overline{\sigma}(i) = \#(\Lambda_i \cup \{i\})$

Observação 2.3.3 *Seja* C *um código e considere o* 1^o *peso generalizado de Hamming:*

$$d_1(C) := min\{\ \#Supp(S) \mid S \text{ é um subcódigo de } C \text{ de dimensão } 1\}$$

Seja S *um subespaço linear de* C *de dimensão* 1*, e seja* $c \neq 0 \in G$*. É fácil ver que* $\#Supp(S) = w(c)$*.*

Assim, como $d(C) = min\{w(c) \mid c \neq 0 \in C\ \}$ *e* $d_1(C) := min\{\ \#Supp(S) = w(c)$ *com* $c \neq 0 \in S \mid$ *onde* S *é um subcódigo de* C *de dimensão* $1\}$*, segue que* $d(C) = d_1(C)$*.*

Observação 2.3.4 *Seja* $G \subseteq B$*, com* $G = \{b_1, b_2, \cdots, b_k\}$*, e seja* $D \subseteq C(B, G)$ *um subespaço de dimensão* t*, com* $t \leq k$*. Então, usando o método de Gauss da álgebra linear (conhecido também como eliminação gaussiana), sempre é possível encontrar uma base* $\{c_1, \cdots, c_t\}$ *para* D *tal que:*

$$c_u = \sum_{s=1}^{k} \alpha_s^{(u)} b_s, \text{ com } u = 1, 2, \cdots, t \quad e \quad máx\{\ s \mid \alpha_s^{(v)} \neq 0\ \} \neq máx\{\ s \mid \alpha_s^{(w)} \neq 0\ \},$$
$$\text{para } \forall v, w \in \{1, \cdots, t\} \text{ com } v \neq w$$

Enfim, a extensão do teorema 2.2.9 para os pesos generalizados de Hamming é:

Teorema 2.3.5 *Seja* $G \subseteq B$ *com* $\#G = k$ *fixada. Então, para* $t = 1, \cdots, k$*:*

$$d_t(C(B, G)) \geq min\{\ \overline{\sigma}(a_1, a_2, \cdots, a_t) \mid 1 \leq a_1 < \cdots < a_t \leq n \ e\ \ \{b_{a_1}, b_{a_2}, \cdots, b_{a_t}\} \subseteq G\ \}.$$

Em particular, a distância mínima de $C(B, G)$ *satisfaz:*

$$d(C(B, G)) \geq min\{\ \overline{\sigma}(i) \mid b_i \in G\ \} = min\{\ \#(\Lambda_i \cup \{i\}) \mid b_i \in G\}$$

Demonstração. Denote $G = \{b_{i_1}, b_{i_2}, \cdots, b_{i_k}\}$ onde $i_1 < i_2 < \cdots < i_k$.

Seja $D \subseteq C(B, G)$ um subespaço de dimensão t, com $t \leq k$. Considere $\{d_1, d_2, \cdots, d_t\}$ como sendo uma base de D. Assim, podemos escrever cada vetor da base de D como uma combinação linear dos vetores da base de G, isto é:

$$d_u = \sum_{s=1}^{k} \alpha_s^{(u)} b_{i_s}, \text{ com } u = 1, 2, \cdots, t.$$

Vamos assumir que:

$$\text{máx}\{\ s \mid \alpha_s^{(v)} \neq 0\ \} \neq \text{máx}\{\ s \mid \alpha_s^{(w)} \neq 0\ \},$$
$$\text{para } \forall v, w \in \{1, \cdots, t\} \text{ com } v \neq w.$$

Se este não for o caso, pela observação (2.3.4) podemos aplicar o método de Gauss no início para achar a partir da base $\{d_1, d_2, \cdots, d_t\}$, uma outra base com esta propriedade.

Por definição, temos que:

$$\overline{\rho}(d_u) = \text{máx}\{\ i_s \mid \alpha_s^{(u)} \neq 0\ \}$$

Logo a afirmação anterior corresponde a assumir que $\overline{\rho}(d_v) \neq \overline{\rho}(d_w)$ para $v \neq w$. Seja $a_u := \overline{\rho}(d_u)$ para $u = 1, 2, \cdots, t$. Observe que se (a_u, j) é WWB para algum
$j \in \{1, 2, \cdots, n\}$ e $\overline{\rho}(b_{a_u} * b_j) = l$, então:

$$\overline{\rho}(d_u * b_j) = \overline{\rho}\left(\left(\sum_{s=1}^{k} \alpha_s^u b_{i_s}\right) * b_j\right) = \overline{\rho}\left(\sum_{s=1}^{k} \alpha_s^u (b_{i_s} * b_j)\right) = \overline{\rho}(b_{a_u} * b_j) = l$$

Consequentemente, o conjunto

$$S := \bigcup_{u=1}^{t} \{\ d_u * b_j \ \mid\ (a_u, j) \text{ é WWB }\}$$

contém pelo menos $\#\ (\bigcup_{u=1}^{t} \Lambda_{a_u})$ vetores L.I.

Considere agora os números a_u, com $u = 1, \cdots, t$. Temos que $a_u = \overline{\rho}(d_u) = \overline{\rho}(d_u * (1, 1, \cdots, 1))$, e portanto o conjunto:

$$S' := \left(\bigcup_{u=1}^{t} \{\ d_u * b_j \ \mid\ (a_u, j)\ WWB\}\right) \cup \{\ d_u * (1, 1, \cdots, 1) \ \mid\ u = 1, \cdots, t\}$$

contém pelo menos $\#\ ((\bigcup_{u=1}^{t} \Lambda_{a_u}) \cup \{a_1, \cdots, a_t\}) = \overline{\sigma}(a_1, \cdots, a_t)$ vetores linearmente independentes.

Consequentemente,

$$\overline{\sigma}(a_1, \cdots, a_t) \leq dim(span_{\mathbb{F}_q}\{\ f \mid f \in S'\ \}). \tag{2.7}$$

Considere a seguir o conjunto:

$$T := \{\ d_u * e \ \mid\ u = 1, \cdots, t \ \ com\ e \in \mathbb{F}_q^n\ \}$$

Veja que o espaço $span_{\mathbb{F}_q}\{\ f \mid f \in T\ \}$ é isomorfo ao espaço $\mathbb{F}_q^{\#Supp(\{d_1, \cdots, d_t\})}$, e como $Supp(D) = Supp(\{d_1, \cdots, d_t\})$ temos que:

$$\#Supp(D) = dim(span_{\mathbb{F}_q}\{\ f \mid f \in T\ \}) \tag{2.8}$$

Mas $S' \subseteq T$, o que implica:

$$dim(span_{\mathbb{F}_q}\{\ f \mid f \in S'\ \}) \leq dim(span_{\mathbb{F}_q}\{\ f \mid f \in T\ \})$$

e usando (2.7) e (2.8), temos:

$$\overline{\sigma}(a_1, \cdots, a_t) \leq \#Supp(D)$$

assim, a prova está concluída. ■

Exemplo 2.3.6 *Seja* $B = \{b_1, b_2\}$ *uma base para* $\mathbb{F}_5^2$ *com* $b_1 = (1, 2)$. *O único par WWB é* $(1, 1)$ *e* $\overline{\rho}(b_1 * b_1) = 2$. *Consequentemente,* $\Lambda_1 = \{2\}$. *Escolha* $G = \{b_1\}$ *e considere o código* $C(B, G)$. *O teorema 2.2.9 nos diz que:*

$$d(C(B, G)) \geq 1$$

enquanto que o teorema 2.3.5 nos diz que:

$$d(C(B, G)) \geq 2$$

Pela cota de Singleton temos que:

$$\begin{gathered} d + k \leq n + 1 \\ d + 1 \leq 2 + 1 \\ d(C(B, G)) \leq 2 \end{gathered}$$

Logo $d(C(B, G)) = 2$, *e a cota do teorema 2.3.5 é atingida.*

Definição 2.3.7 *Seja* $B = \{b_1, b_2, \cdots, b_n\}$ *uma base para* $\mathbb{F}_q^n$. *Para* $s = 1, 2, \cdots, n$ *e* $\delta = 0, 1, \cdots, n$ *definimos:*

$$\varepsilon(s) := span_{\mathbb{F}_q}\{b_1, b_2, \cdots, b_s\}$$

$$\tilde{\varepsilon}(\delta) := span_{\mathbb{F}_q}\{\ b_i \mid \overline{\sigma}(i) \geq \delta\ \}$$

Do nosso exemplo motivador podemos ver que é bem natural considerarmos os códigos de Reed-Solomon como sendo códigos da forma $\varepsilon(s)$.

Veremos a frente que também será natural considerarmos os códigos geométricos de Goppa como sendo da forma $\varepsilon(s)$. A seguir, temos o seguinte teorema:

Teorema 2.3.8 *A distância mínima de* $\varepsilon(s)$ *e a distância mínima de* $\tilde{\varepsilon}(\delta)$ *satisfazem:*

$$d(\varepsilon(s)) \geq min\{\ \overline{\sigma}(i) \mid i = 1, \cdots, s\ \}$$

$$\tilde{\varepsilon}(\delta) \geq \delta$$

Demonstração. Temos que $\varepsilon(s) = C(B, G)$ com $G = \{b_1, \cdots, b_s\}$ e temos que $\tilde{\varepsilon}(\delta) = C(B, G)$ com $G = \{\ b_i \mid \overline{\sigma}(i) \geq \delta\ \}$. O resultado agora segue pelo teorema 2.3.5. ■

2.4 A cota de Feng-Rao para os pesos generalizados de Hamming

A cota no teorema 2.3.5 é semelhante a cota de Feng-Rao para os códigos $C^{\perp}(B, G)$. Veremos isto, mas antes precisaremos de algumas definições.

Definição 2.4.1 *Para* $l = 1, \cdots, n$ *seja*

$$V_l := \{i \in I_n \ \mid\ \overline{\rho}(b_i * b_j) = l \text{ para algum } b_j \in B \text{ com } (i, j) \text{ WWB }\}$$

Para $\{l_1, l_2, \cdots, l_t\} \subset I_n$ *definimos*

$$\overline{\mu}(l_1, l_2, \cdots, l_t) := \sharp\left(\left(\bigcup_{s=1}^{t} V_{l_s}\right) \cup \{l_1, \cdots, l_t\}\right)$$

Em particular, definimos

$$\overline{\mu}(l) := \sharp(V_l \cup \{l\})$$

Exemplo 2.4.2 *Considere* $B = \{b_1 = (1,0,2,4,3) \ ; \ b_2 = (2,1,3,0,1) \ ; \ b_3 = (0,2,1,2,4) \ ; \ b_4 = (1,3,0,1,2) \ ; \ b_5 = (1,2,4,3,0)\}$ *como uma base de* $\mathbb{F}_5^5$. *Depois de alguns cálculos, temos que os únicos pares* (i,j) *WWB são:*

(1,1), (1,2), (1,3), (2,1), (3,1)

e ainda temos que

$$\begin{gathered}\overline{\rho}(b_1 * b_1) = 3 \\ \overline{\rho}(b_1 * b_2) = \overline{\rho}(b_2 * b_1) = 4 \\ \overline{\rho}(b_1 * b_3) = \overline{\rho}(b_3 * b_1) = 5\end{gathered}$$

Assim, temos por exemplo que:

$$V_4 = \{i \in I \ \mid \ \overline{\rho}(b_i * b_j) = 4 \text{ para algum } b_j \in B \text{ com } (i,j) \text{ WWB } \} = \{1,2\}$$

Da mesma forma:

$$\begin{gathered}V_1 = V_2 = \emptyset \\ \text{e } V_3 = \{1\} \text{ e } V_5 = \{1,3\}\end{gathered}$$

Logo temos que

$$\overline{\mu}(1,4,5) = \sharp\left(\left(\bigcup_{s=1,4,5} V_{l_s}\right) \cup \{1,4,5\}\right) = \sharp(\{1,2,3,4,5\}) = 5$$

Podemos agora enunciar a cota de Feng-Rao para os pesos generalizados de Hamming. Esta formulação é relativamente parecida com a formulação original dada por Feng e Rao com relação à distância mínima.

Teorema 2.4.3 ***(A cota de Feng-Rao)*** *O t-ésimo peso generalizado de Hamming* $d_t(C^{\perp}(B,G))$ *satisfaz:*

$$d_t(C^{\perp}(B,G)) \geq min\{ \ \overline{\mu}(\ a_1, \cdots, a_t) \mid a_i \neq a_j \text{ para } i \neq j \ \ e \ \ \{b_{a_1}, \cdots, b_{a_t}\} \subseteq B \setminus G\}$$

Em particular,

$$d(C^{\perp}(B,G)) \geq \ min \ \{ \ \overline{\mu}(a) \mid b_a \in B \setminus G\}$$

Demonstração. Uma prova deste teorema pode ser encontrada na referência [10]. ■

Nas seções que virão a seguir vamos precisar dos seguintes códigos:

Definição 2.4.4 *Dada uma base* $B = \{b_1, \cdots, b_n\}$, *definimos*

$$\begin{gathered}\mathcal{C}(s) := C^{\perp}(B,G), \text{ com } G = \{b_1, \cdots, b_s\} \\ \tilde{\mathcal{C}}(\delta) := C^{\perp}(B,G), \text{ com } G = \{ \ b_i \in B \mid \overline{\mu}(i) < \delta\}\end{gathered}$$

Podemos aplicar a cota de Feng-Rao nos códigos $\mathcal{C}(s)$ e $\tilde{\mathcal{C}}(\delta)$.

Em particular,

$$d(\tilde{\mathcal{C}}(\delta)) \geq \ \ min \ \{ \ \overline{\mu}(a) \mid b_a \in B \setminus \{ \ b_i \mid \overline{\mu}(i) < \delta \ \}\} \geq \delta$$

Assim, os códigos $\tilde{\mathcal{C}}(\delta)$ são frequentemente chamados *códigos duais melhorados* ou *códigos melhorados de Feng-Rao.*

2.5 Uma conexão com o trabalho de Shibuya e Sakaniwa

Na referência [7], Shibuya e Sakaniwa encontraram uma cota para a distância mínima para os códigos $C(B,G)$. Vamos ver a seguir que existe uma forte conexão entre o teorema 2.3.5 e a cota de Shibuya e Sakaniwa.

Recorde que

$$\Lambda_i := \{\ l \in I_n \ \mid\ \overline{\rho}(b_i * b_j) = l \text{ para algum } b_j \text{ com } (i,j) \text{ WWB }\}$$

Vamos enunciar a cota de Shibuya e Sakaniwa.

Teorema 2.5.1 ***(A cota de Shibuya e Sakaniwa)***. *Dada uma base $B = \{b_1, b_2, \cdots, b_n\}$ e $G \subseteq B$, seja $T_i := \{v \in I \mid b_v \in B \setminus G\} \setminus \Lambda_i$, para $i = 1, 2, \cdots, n$. Definimos $t(B,G) := max\{\ \sharp(T_i) \mid b_i \in G\}$. A distância mínima de $C(B,G)$ satisfaz:*

$$d(C(B,G)) \geq n - k + 1 - t(B,G)$$

Demonstração. Uma prova deste resultado pode ser encontrada na referência [7]. ■

Vamos mostrar agora como a cota de Shibuya e Sakaniwa pode ser vista como uma consequência do teorema 2.3.5.

Teorema 2.5.2 *A cota da distância mínima de $C(B,G)$ no teorema 2.3.5 é maior ou igual à cota de Shibuya e Sakaniwa.*

Demonstração. Seja $B = \{b_1, b_2, \cdots, b_n\}$ e $G = \{b_{l_1}, b_{l_2}, \cdots, b_{l_k}\} \subseteq B$. Para $i = 1, \cdots, k$, temos que:

$$\overline{\sigma}(l_i) = \sharp(\Lambda_{l_i} \cup \{l_i\})$$

Para cada $l_i \in \{l_1, l_2, \cdots, l_k\}$, o conjunto T_{l_i} consiste de todos os números $v \in I_n$ tais que $b_v \in B \setminus G$ e que não contribuem para a contagem dos elementos do conjunto $\Lambda_{l_i} \cup \{l_i\}$.

Consequentemente, a quantidade de números de elementos $v \in I_n$ com $b_v \in B \setminus G$ e que não contribuem para a contagem dos elementos do conjunto $\Lambda_{l_i} \cup \{l_i\}$ é $n - k - \sharp(T_{l_i})$.

Para cada $l_i \in \{l_1, l_2, \cdots, l_k\}$, o número de elementos $v \in I$ com $b_v \in G$ e que contribuem para a contagem dos elementos do conjunto $\Lambda_{l_i} \cup \{l_i\}$ é maior ou igual a $\sharp(\{l_i\}) = 1$.

Assim, $n - k + 1 - \sharp(T_i) \leq \sharp(\Lambda_i \cup \{i\}) = \overline{\sigma}(i)$ para todo i com $b_i \in G$, e o resultado segue. ■

Observação 2.5.3 *Note que T_i depende da escolha de G. Isto significa que os cálculos feitos para uma escolha de G não podem ser reutilizados para outra escolha de G. Em particular, dada uma base B não é tão fácil ver qual deve ser a melhor escolha de G. As vantagens do teorema 2.3.5 em comparação com a cota de Shibuya e Sakaniwa são as seguintes:*

Primeiramente, o teorema 2.3.5 é muito mais simples de implementar, e no caso da distância mínima a prova é quase trivial.

Depois, os cálculos feitos para uma escolha de G podem ser reusados para outras escolhas de G. Como uma consequencia, o teorema 2.3.5 nos permite construir códigos melhorados $\tilde{\varepsilon}(\delta)$.

Ainda temos que o teorema 2.3.5 trata não somente da distância mínima mas também de todos os pesos generalizados de Hamming. Finalmente, usando o teorema 2.3.5 podemos definir e lidar com códigos vindos da teoria de domínios de ordem.

Capítulo 3

Domínios de Ordem

3.1 Códigos da teoria de domínios de ordem

Nas seções anteriores vimos como estimar os parâmetros de qualquer código linear, mas para que esse método seja realmente prático precisaremos de bases $B = \{b_1, \cdots, b_n\}$ para $\mathbb{F}_q^n$ tais que seja fácil decidir se um dado par (i, j) é WB(ou WWB) e também seja fácil calcular $\overline{\rho}(b_i * b_j)$.

Uma maneira de encontrar tais bases é usando a teoria de domínios de ordem que vamos apresentar a seguir. Recorde do exemplo motivador como os códigos de Reed-Solomon foram vistos como a imagem de um subespaço do anel de polinômios $R = \mathbb{F}_q[X]$ pela aplicação de avaliação $ev : \mathbb{F}_q[X] \to \mathbb{F}_q^n$. Recorde também como usamos a função grau em $\mathbb{F}_q[X]$ para decidir o valor de $\overline{\rho}(c * b_j)$. A idéia da teoria dos domínios de ordem é generalizar este contexto para uma classe maior de estruturas algébricas chamadas **domínios de ordem**.

Vamos enunciar o conceito de ordem monomial sobre $\mathbb{F}[X_1, \cdots, X_n]$.

Definição 3.1.1 *Uma **ordem monomial** sobre $\mathbb{F}[X_1, \cdots, X_n]$ é uma relação $\prec$ sobre $\mathbb{N}_0^r$, ou equivalentemente, uma relação sobre o conjunto de todos os monômios nas variáveis $X_1, \cdots, X_n$, que satisfaz:*
(a) $\prec$ é uma ordem total sobre $\mathbb{N}_0^r$.
(b) Se $\alpha \prec \beta$ e $\gamma \in \mathbb{N}_0^r$, então $\alpha + \gamma \prec \beta + \gamma$.
(c) $\prec$ é uma boa-ordem sobre $\mathbb{N}_0^r$. Isto significa que todo subconjunto não vazio de $\mathbb{N}_0^r$ possui um menor elemento em relação a $\prec$.

Definição 3.1.2 *Seja R uma $\mathbb{F}_q$-álgebra e seja Γ um subsemigrupo de $\mathbb{N}_0^r$ para algum r. Seja $\prec$ uma ordem monomial sobre $\mathbb{N}_0^r$. Uma aplicação sobrejetora $\rho : R \to \Gamma_{-\infty} := \Gamma \cup \{-\infty\}$ que satisfaz as seis seguintes condições é dita ser uma função peso.*

(W.0) $\rho(f) = -\infty \iff f = 0$.
(W.1) $\rho(af) = \rho(f)$ para todo $a \in \mathbb{F}_q$ não nulo.
(W.2) $\rho(f + g) \preceq max\{\rho(f), \rho(g)\}$ e a igualdade ocorre quando $\rho(f) \prec \rho(g)$.
(W.3) Se $\rho(f) \prec \rho(g)$ e $h \neq 0$, então $\rho(fh) \prec \rho(gh)$.
(W.4) Se f e g são não nulos e $\rho(f) = \rho(g)$, então existe um $a \in \mathbb{F}_q$ não nulo, tal que $\rho(f - ag) \prec \rho(g)$.
(W.5) Se f e g são não nulos, então $\rho(fg) = \rho(f) + \rho(g)$.

*Uma $\mathbb{F}_q$-álgebra com uma função peso é chamada de **domínio de ordem sobre** $\mathbb{F}_q$. A terna (R, ρ, Γ) é chamada de **estrutura de ordem**, e Γ é chamado de **semigrupo de valores de** ρ.*

Teorema 3.1.3 *Seja (R, ρ, Γ) uma estrutura de ordem sobre $\mathbb{F}_q$. Seja $\beta = \{f_\alpha \mid \alpha \in \Gamma\}$ uma sequência de elementos em R tais que $\rho(f_\alpha) = \alpha$ para todo $\alpha \in \Gamma$. Então $\{f_\alpha \mid \alpha \in \Gamma\}$ é uma base para R como espaço vetorial sobre $\mathbb{F}_q$. Em particular, $\{f_\alpha \in \beta \mid \alpha \preceq \gamma\}$ é uma base para $R_\gamma := \{f \in R \mid \rho(f) \preceq \gamma\}$.*

Demonstração. Seja $\{f_{\alpha_1}, f_{\alpha_2}, \cdots, f_{\alpha_m}\} \subset \{f_\alpha \mid \alpha \in \Gamma\}$ com $\alpha_i \neq \alpha_j$ *para* $i \neq j$. Considere uma $\mathbb{F}_q-$combinação linear $a_1 f_{\alpha_1} + \cdots + a_m f_{\alpha_m} = 0$. Aplicando a função ρ temos que $\rho(a_1 f_{\alpha_1} + \cdots + a_m f_{\alpha_m}) = \rho(0) = -\infty$, mas como $f_{\alpha_1}, \cdots, f_{\alpha_m}$ são distintos temos que $\rho(a_1 f_{\alpha_1} + \cdots + a_m f_{\alpha_m}) = max\{\rho(a_1 f_{\alpha_1}), \cdots, \rho(a_m f_{\alpha_m})\} = \rho(a_j f_{\alpha_j})$ para algum j. Logo, $\rho(a_j f_{\alpha_j}) = -\infty$ nos diz que $a_j = 0$. Repetindo este processo, temos que $a_i = 0$ para $i = 1, \cdots, m$, e portanto $\{f_{\alpha_1}, f_{\alpha_2}, \cdots, f_{\alpha_m}\}$ é linearmente independente.

Agora seja $f \neq 0 \in R$, logo existe $f_{\alpha_1} \in \{f_\alpha \mid \alpha \in \Gamma\}$ tal que $\rho(f_{\alpha_1}) = \rho(f)$. Por (W.4) existe $a_1 \neq 0 \in \mathbb{F}_q$ tal que $\rho(f - a f_{\alpha_1}) \prec \rho(f_{\alpha_1})$. Se $\rho(f - a_1 f_{\alpha_1}) = -\infty$ acabou. Caso contrário, existe $f_{\alpha_2} \in \{f_\alpha \mid \alpha \in \Gamma\}$ tal que $\rho(f_{\alpha_2}) = \rho(f - a_1 f_{\alpha_1})$, mas por (W.4) existe $a_2 \neq 0 \in \mathbb{F}_q$ tal que $\rho((f - a_1 f_{\alpha_1}) - a_2 f_{\alpha_2}) \prec \rho(f_{\alpha_2})$. Se $\rho(f - a_1 f_{\alpha_2} - a_2 f_{\alpha_2}) = -\infty$ acabou.

Caso contrário, repetimos este processo novamente. Agora note que a sequência:

$$(\alpha) := \alpha_1 \succ \alpha_2 \succ \alpha_3 \succ \cdots$$

é uma sequência (não necessariamente infinita) estritamente decrescente de elementos de $\Gamma \subseteq \mathbb{N}_0^r$. Como $\prec$ é uma ordem monomial sobre $\mathbb{N}_0^r$, logo $\prec$ é uma boa ordem sobre $\mathbb{N}_0^r$, então segue que a sequência (α) eventualmente termina, isto é; existe $m \in \mathbb{N}$ tal que $(\alpha) = \alpha_1 \succ \alpha_2 \succ \cdots \succ \alpha_m$.
Assim, após repetirmos este processo m vezes, obtemos:

$$\rho(f - a_1 f_{\alpha_1} - a_2 f_{\alpha_2} - \cdots - a_m f_{\alpha_m}) = -\infty.$$

o que nos diz que $f = a_1 f_{\alpha_1} + \cdots + a_m f_{\alpha_m}$. ■

Uma base β como no teorema acima, é chamada de **base bem-comportada**.

Exemplo 3.1.4 *Considere o anel quociente $R := \mathbb{F}_9[X, Y]/I$ onde I é o ideal gerado pelo polinômio Hermitiano $X^4 - Y^3 - Y$. Mais adiante, vamos ver que o conjunto:*

$$\{X^\alpha Y^\beta + I \mid 0 \leq \alpha,\ 0 \leq \beta < 3\}$$

é uma base para R como espaço vetorial sobre $\mathbb{F}_9$.

Agora, vamos definir $\rho(X^\alpha Y^\beta + I) := 3\alpha + 4\beta$ para $0 \leq \alpha$ e $0 \leq \beta < 3$. Assim, ρ está definida sobre todo elemento de nossa base. Usando as propriedades (W.0),(W.1) e (W.2) ρ é extendida para todo R. Temos que $\Gamma = \langle 3, 4\rangle$ (aqui $\langle s_1, \cdots, s_r\rangle$ significa o semigrupo gerado por $s_1, \cdots, s_r$).

A base no exemplo 3.1.4 é um exemplo de uma base bem comportada para o domínio de ordem R.

Segue abaixo uma tabela (tabela 3.1) mostrando os valores de ρ para alguns elementos de $\{X^\alpha Y^\beta + I \mid 0 \leq \alpha,\ 0 \leq \beta < 3\}$.

Y^2	XY^2	X^2Y^2	X^3Y^2	X^4Y^2	X^5Y^2	X^6Y^2	X^7Y^2	X^8Y^2	X^9Y^2	$\cdots$
Y	XY	X^2Y	X^3Y	X^4Y	X^5Y	X^6Y	X^7Y	X^8Y	X^9Y	$\cdots$
1	X	X^2	X^3	X^4	X^5	X^6	X^7	X^8	X^9	$\cdots$
8	11	14	17	20	23	26	29	32	35	$\cdots$
4	7	10	13	16	19	22	25	28	31	$\cdots$
0	3	6	9	12	15	18	21	24	27	$\cdots$

Tabela 3.1: Valores de ρ do exemplo 3.1.4.

Definição 3.1.5 *Seja R uma $\mathbb{F}_q$-álgebra. Uma aplicação sobrejetora $\varphi : R \to \mathbb{F}_q^n$ é chamada de* ***homomorfismo de $\mathbb{F}_q$-álgebras*** *se φ é $\mathbb{F}_q$-linear e $\varphi(fg) = \varphi(f) * \varphi(g)$ para todo $f, g \in R$.*

Agora é natural tomar elementos na base $B = \{b_1, \cdots, b_n\}$ para $\mathbb{F}_q^n$ como sendo da forma $\varphi(f_\lambda)$ para n diferentes valores de λ.

Vamos ver que os valores $\alpha(1), \cdots, \alpha(n)$ na próxima definição serão uma boa escolha para os $\lambda' s$.

Definição 3.1.6 *Seja $\alpha(1) := 0$. Para $i = 2, 3, \cdots, n$ definimos $\alpha(i)$ recursivamente como sendo o menor elemento em Γ que é maior que $\alpha(1), \alpha(2), \cdots, \alpha(i-1)$ e satisfaz $\varphi(R_\gamma) \subsetneqq \varphi(R_{\alpha(i)})$ para todo $\gamma \prec \alpha(i)$.*

Notação: $\{\alpha(1), \alpha(2), \cdots, \alpha(n)\} = \Delta(R, \rho, \varphi)$.

Observação 3.1.7 *Veja que a definição de $\Delta(R, \rho, \varphi)$ acima está bem definida, isto é; dado um homomorfismo de $\mathbb{F}_q$-álgebras $\varphi : R \to \mathbb{F}_q^n$ existem realmente n elementos em $\Delta(R, \rho, \varphi)$.*

De fato, como φ é sobrejetora podemos considerar o seguinte conjunto não vazio abaixo:

$$A_2 := \{\alpha \in \Gamma \mid 0 \prec \alpha \text{ e } \{\varphi(f_{\alpha(1)}), \varphi(f_\alpha)\} \text{ é L.I. } \}$$

(onde L.I. significa linearmente independente).

Veja que $A_2 \subseteq \mathbb{N}_0^r$, e como $\prec$ é uma ordem monomial sobre $\mathbb{N}_0^r$ logo existe $\alpha_2 \in A_2$ tal que $\alpha_2 \preceq \alpha$, $\forall \alpha \in A_2$. É fácil ver que α_2 é o menor elemento em Γ que é maior que 0 e $\varphi(R_\gamma) \subsetneqq \varphi(R_{\alpha_2})$ para todo $\gamma \prec \alpha_2$.

Assim, $\alpha_2 = \alpha(2) \in \Delta(R, \rho, \varphi)$. Novamente, podemos considerar o conjunto:

$$A_3 := \{\alpha \in \Gamma \mid 0 \prec \alpha_2 \prec \alpha \text{ e } \{\varphi(f_{\alpha(1)}), \varphi(f_{\alpha(2)}), \varphi(f_\alpha)\} \text{ é L.I. } \}$$

E novamente existe $\alpha_3 \in A_3$ tal que $\alpha_3 \preceq \alpha$, $\forall \alpha \in A_3$, e seguindo o mesmo raciocínio temos que $\alpha_3 = \alpha(3) \in \Delta(R, \rho, \varphi)$. Assim, podemos repetir este processo criando recursivamente os conjuntos $A_4, \cdots, A_n$ e obtendo $\alpha(4), \cdots, \alpha(n) \in \Delta(R, \rho, \varphi)$.

O seguinte teorema é facilmente provado.

Teorema 3.1.8 *Seja $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \cdots, \alpha(n)\}$ como na definição 3.1.6. O conjunto*

$$B := \{\ b_1 := \varphi(f_{\alpha(1)}),\ b_2 := \varphi(f_{\alpha(2)}),\ \cdots\ ,\ b_n := \varphi(f_{\alpha(n)})\}$$

é uma base para $\mathbb{F}_q^n$ *como espaço vetorial sobre* $\mathbb{F}_q$.

Para qualquer $c \in \mathbb{F}_q^n$ *existe um único conjunto ordenado* $(\beta_1, \beta_2, \cdots, \beta_n)$, *com* $\beta_i \in \mathbb{F}_q$ *para* $i = 1, \cdots, n$ *tal que* $c = \varphi\left(\sum_{i=1}^{n} \beta_i f_{\alpha(i)}\right)$.
A função $\overline{\rho} : \mathbb{F}_q^n \to \{0, 1, \cdots, n\}$ *correspondente a base* B *é dada por:*

$$\overline{\rho}(c) = \begin{cases} 0, & se\ c = 0, \\ max\{i \mid \beta_i \neq 0\}, & se\ c \neq 0 \end{cases}$$

Demonstração. Como $dim\ (\mathbb{F}_q^n) = n$, só precisaremos mostrar que B é um conjunto linearmente independente. Para cada $i = 1, \cdots, n$ temos que:

$$\varphi(f_{\alpha_i}) \in \varphi(R_{\alpha_i}) \setminus \varphi(R_{\alpha_i - 1})$$

Logo,

$$\begin{array}{c} b_1 \in \varphi(R_{\alpha_{(1)}}) = \varphi(R_0) \\ b_2 \in \varphi(R_{\alpha_{(2)}}) \backslash \varphi(R_{\alpha_{(1)}}) \\ \vdots \quad \vdots \\ b_n \in \varphi(R_{\alpha_{(n)}}) \backslash \varphi(R_{\alpha_{(n-1)}}) \end{array}$$

e como $\varphi(R_{\alpha_{(1)}}) \subsetneqq \cdots \subsetneqq \varphi(f_{\alpha_{(n)}}) = \mathbb{F}_q^n$, segue que $\{b_1, \cdots, b_n\}$ é linearmente independente. As demais afirmações são facilmente mostradas. ■

Proposição 3.1.9 *Seja* P *o conjunto formado pelos distintos pontos* $P_1, \cdots, P_n$ *em* $\mathbb{F}_q^m$. *Seja* $R = \mathbb{F}_q[X_1, \cdots, X_m]$. *Considere a aplicação de avaliação:*

$$ev_P : R \to \mathbb{F}_q^n$$

definida por $ev_p(f) = (f(P_1), \cdots, f(P_n))$. *Então a aplicação* ev_P *é um homomorfismo de* $\mathbb{F}_q$ *- álgebras.*

Demonstração. Vamos mostrar que ev_P é sobrejetora. Seja $P_j = (x_{j1}, \cdots, x_{jm})$. Seja $A_{il} = \{x_{jl} \mid j = 1, \cdots, n\} \setminus \{x_{il}\}$. Defina o polinômio G_i por:

$$G_i = \prod_{l=1}^{m} \prod_{x \in A_{il}} (X_l - x)$$

Então $G_i(P_j) = 0$ para todo $i \neq j$. Ainda mais, $G_i(P_i) \neq 0$, já que $P_1, \cdots, P_n$ são distintos. O polinômio $\dfrac{G_i}{G(P_i)}$ é levado pela aplicação ev_P no i-ésimo elemento da base canônica de $\mathbb{F}_q^n$. Consequentemente ev_P é sobrejetora. É fácil ver que ev_P é linear e que $ev_P(fg) = ev_P(f) * ev_P(g)$ para $\forall f, g \in R$, logo ev_P é um homomorfismo. ■

Observação 3.1.10 *Suponha que* I *é um ideal no anel* $\mathbb{F}_q[X_1, \cdots, X_m]$. *Seja* $V = \{P_1, \cdots, P_n\}$ *o conjunto de zeros de* I *com coordenadas em* $\mathbb{F}_q$, *isto é;* $V = \{P \in \mathbb{F}_q^n \mid f(P) = 0\ para\ \forall f \in I$. *Então a aplicação* ev_P *acima induz uma outra aplicação linear bem definida:*

$$\varphi : \mathbb{F}_q[X_1, \cdots, X_m] \diagup I \to \mathbb{F}_q^n$$

definida por $\varphi(f+I) = (f(P_1), \cdots, f(P_n))$ *que também é um homomorfismo de* $\mathbb{F}_q$ *- álgebras.*

Exemplo 3.1.11 *Vamos continuar o exemplo 3.1.4. O polinômio hermitiano* $X^4 - Y^3 - Y$ *tem 27 zeros* $P_1, \cdots, P_{27}$*.*

Denotando $\mathbb{F}_9 = \{0, 1, 2, \alpha, 1+\alpha, 2+\alpha, 2\alpha, 1+2\alpha, 2+2\alpha\}$ *onde* $\alpha^2 + 1 = 0$*, temos que os 27 zeros são:*

$$\begin{bmatrix} P_1 = (0,0) & P_2 = (0,\alpha) & P_3 = (0,2\alpha) \\ P_4 = (1,2) & P_5 = (1,2+\alpha) & P_6 = (1,2+2\alpha) \\ P_7 = (2,2) & P_8 = (2,2+\alpha) & P_9 = (2,2+2\alpha) \\ P_{10} = (\alpha,2) & P_{11} = (\alpha,2+\alpha) & P_{12} = (\alpha,2+2\alpha) \\ P_{13} = (2\alpha,2) & P_{14} = (2\alpha,2+\alpha) & P_{15} = (2\alpha,2+2\alpha) \\ P_{16} = (1+\alpha,1) & P_{17} = (1+\alpha,1+\alpha) & P_{18} = (1+\alpha,1+2\alpha) \\ P_{19} = (2+\alpha,1) & P_{20} = (2+\alpha,1+\alpha) & P_{21} = (2+\alpha,1+2\alpha) \\ P_{22} = (1+2\alpha,1) & P_{23} = (1+2\alpha,1+\alpha) & P_{24} = (1+2\alpha,1+2\alpha) \\ P_{25} = (2+2\alpha,1) & P_{26} = (2+2\alpha,1+\alpha) & P_{27} = (2+2\alpha,1+2\alpha) \end{bmatrix}$$

Definindo uma função $\varphi : R \to \mathbb{F}_9^{27}$ *por*

$$\varphi(F(X,Y) + I) := (F(P_1), \cdots, F(P_{27})).$$

Pela observação 3.1.10, temos que φ *é um homomorfismo de* $\mathbb{F}_q$ *- álgebras.*

Por inspeção, temos que para $0 \leq \alpha < 9$ *e* $0 \leq \beta < 3$

$$\varphi(X^\alpha Y^\beta + I) \in \varphi(R_{3\alpha+4\beta}) \setminus \varphi(R_{3\alpha+4\beta-1})$$

Portanto

$$\Delta(R, \rho, \varphi) = \{3\alpha + 4\beta \mid 0 \leq \alpha < 9,\ 0 \leq \beta < 3\}.$$

Denotando para $i = 1, \cdots, 27$*,* $f_{\alpha(i)} = F(i) + I$*, temos a tabela abaixo:*

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\alpha(i)$	0	3	4	6	7	8	9	10	11	12	13	14	15	16
$F(i)$	1	X	Y	X^2	XY	Y^2	X^3	X^2Y	XY^2	X^4	X^3Y	X^2Y^2	X^5	X^4Y
i	15	16	17	18	19	20	21	22	23	24	25	26	27	
$\alpha(i)$	17	18	19	20	21	22	23	24	25	26	28	29	32	
$F(i)$	X^3Y^2	X^6	X^5Y	X^4Y^2	X^7	X^6Y	X^5Y^2	X^8	X^7Y	X^6Y^2	X^8Y	X^7Y^2	X^8Y^2	

Tabela 3.2: Valores de $\alpha(i)$.

Mas adiante, vamos ver uma outra maneira de encontrar o conjunto $\Delta(R, \rho, \varphi)$ sem recorermos a fazer a inspeção acima, o que é de fato um árduo trabalho.

De agora em diante, vamos assumir sempre que a base $B = \{b_1, \cdots, b_n\}$ é da mesma forma da base B no teorema 3.1.8.

Gostaríamos de saber quais pares $(i,j) \in I^2$ são WB e de encontrar qual é o valor de $\overline{\rho}(b_i * b_j)$. As duas proposições seguintes vão nos ajudar a responder em parte estas questões.

Proposição 3.1.12 *Seja* $B = \{b_1, \cdots, b_n\}$ *uma base como em 3.1.8. Se* $\alpha(i), \alpha(j), \alpha(l) \in \Delta(R, \rho, \varphi)$ *são tais que* $\alpha(i) + \alpha(j) = \alpha(l)$*, então* $\overline{\rho}(b_i * b_j) = l$ *e* $(i,j) \in I_n^2$ *é WB.*

Demonstração. Vamos mostrar primeiro que $\overline{\rho}(b_i * b_j) = l$. Temos por hipótese que:

$$\alpha(i) + \alpha(j) = \alpha(l) \Rightarrow \rho(f_{\alpha(i)}) + \rho(f_{\alpha(j)}) = \alpha(l)$$

Por (W.5) temos que

$$\alpha(l) = \rho(f_{\alpha(i)}) + \rho(f_{\alpha(j)}) = \rho(f_{\alpha(i)} \cdot f_{\alpha(j)})$$

Logo $f_{\alpha(i)} \cdot f_{\alpha(j)} \in \{f \in R \mid \rho(f) \leq \alpha(l)\} = R_{\alpha(l)}$ e $f_{\alpha(i)} \cdot f_{\alpha(j)} \notin \{f \in R \mid \rho(f) \leq \gamma\} = R_\gamma$, $\forall \gamma < \alpha(l)$. Assim $\varphi(f_{\alpha(i)} \cdot f_{\alpha(j)}) \in \varphi(R_{\alpha(l)}) = \varphi(\{f \in R \mid \rho(f) \leq \alpha(l)\}) = L_l$ e $\varphi(f_{\alpha(i)} \cdot f_{\alpha(j)}) \notin L_w$ para $\forall w < l$. Logo, $\varphi(f_{\alpha(i)} \cdot f_{\alpha(j)}) \in L_l \setminus L_{l-1}$. Mas $\varphi(f_{\alpha(i)} \cdot f_{\alpha(j)}) = \varphi(f_{\alpha(i)}) * \varphi(f_{\alpha(j)}) = b_i * b_j$. Assim, $b_i * b_j \in L_l \setminus L_{l-1} \Rightarrow \overline{\rho}(b_i * b_j) = l$.

Agora vamos mostrar que (i, j) é WB. Sejam $u, v \in I_n$ tais que $1 \leq u \leq i$, $1 \leq v \leq j$ e $(u, v) \neq (i, j)$. Temos que $\alpha(u) < \alpha(i)$ ou $\alpha(v) < \alpha(j)$. Suponha que $\alpha(u) < \alpha(i)$, o outro caso é análogo. Logo, $\rho(f_{\alpha(u)}) < \rho(f_{\alpha(i)})$ e como $f_{\alpha(v)} \neq 0$, por (W.3) temos que:

$$\begin{aligned}\rho(f_{\alpha(u)} \cdot f_{\alpha(v)}) &< \rho(f_{\alpha(i)} \cdot f_{\alpha(v)}) = \rho(f_{\alpha(i)}) + \rho(f_{\alpha(v)}) \\ &\leq \rho(f_{\alpha(i)}) + \rho(f_{\alpha(j)}) = \rho(f_{\alpha(i)} f_{\alpha(j)}) = \alpha(l)\end{aligned}$$

Logo, pelas definições 3.1.5 e 3.1.6 temos:

$$b_u * b_v = \varphi(f_{\alpha(u)}) * \varphi(f_{\alpha(v)}) = \varphi(f_{\alpha(u)} f_{\alpha(v)}) \in \varphi(R_\gamma) \text{ para algum } \gamma < \alpha(l).$$

Logo $b_u * b_v \in \varphi(R_\gamma) \subseteq L_{l-1}$. Isto implica que $\overline{\rho}(b_u * b_v) \leq l - 1$ e consequentemente (i, j) é WB. ■

Proposição 3.1.13 *Considere $\alpha(l) \in \Delta(R, \rho, \varphi)$ e assuma que existem $\beta_1, \beta_2 \in \Gamma$ tais que $\beta_1 + \beta_2 = \alpha(l)$. Então $\beta_1, \beta_2 \in \Delta(R, \rho, \varphi)$.*

Demonstração. Temos que $\beta_1 + \beta_2 = \rho(f_{\beta_1}) + \rho(f_{\beta_2}) = \rho(f_{\beta_1} f_{\beta_2})$, logo $f_{\beta_1} f_{\beta_2} \in R_{\alpha(l)}$ e $f_{\beta_1} f_{\beta_2} \notin R_\gamma$ para qualquer $\gamma < \alpha(l)$. Vamos mostrar que $\beta_1 \in \Delta(R, \rho, \varphi)$, a demonstração para β_2 será análoga.

Suponha por absurdo que $\beta_1 \notin \Delta(R, \rho, \varphi)$, isto é, que existe $w \in \Gamma$ tal que $w < \beta_1$ e $\varphi(R_w) = \varphi(R_{\beta_1})$. Em particular, temos que $\varphi(f_{\beta_1}) \in \varphi(R_w)$. Assim, existe $g \in R_w$ com $\varphi(g) = \varphi(f_{\beta_1})$ o que implica $\varphi(g f_{\beta_2}) = \varphi(f_{\beta_1} f_{\beta_2})$.

Como $g \in R_w$, logo $\rho(g) \leq w < \beta_1$, o que nos diz que $\rho(g) < \rho(f_{\beta_1})$. Como $f_{\beta_2} \neq 0$, por (W.3) temos que

$$\rho(g f_{\beta_2}) < \rho(f_{\beta_1} f_{\beta_2}) = \alpha(l)$$

Denotando por $\gamma_0 = \rho(g f_{\beta_2})$, note que $g f_{\beta_2} \in R_{\gamma_0}$ e logo $\varphi(g f_{\beta_2}) \in \varphi(R_{\gamma_0})$, mas $\varphi(g f_{\beta_2}) = \varphi(f_{\beta_1} f_{\beta_2})$ logo $\varphi(f_{\beta_1} f_{\beta_2}) \in \varphi(R_{\gamma_0})$ e $\gamma_0 < \alpha(l)$, o que é uma contradição pois $f_{\beta_1} f_{\beta_2} \in R_{\alpha(l)}$ e $f_{\beta_1} f_{\beta_2} \notin R_\gamma$ para qualquer $\gamma < \alpha(l)$. ■

Note que com as duas proposições acima em mãos podemos estimar facilmente os valores de $\overline{\sigma}(i)$ e $\overline{\mu}(i)$ para $i = 1, \cdots, n$.

Definição 3.1.14 *(a) Para $\eta \in \Delta(R, \rho, \varphi) = \{\alpha(1), \cdots, \alpha(n)\}$ definimos:*

$$M(\eta) := \{\gamma \in \Delta(R,\rho,\varphi) \mid \exists\ \beta \in \Delta(R,\rho,\varphi)\ com\ \eta+\beta=\gamma\}$$
$$= (\eta+\Gamma)\cap\Delta(R,\rho,\varphi).$$

onde $\eta+\Gamma$ *significa* $\{\eta+\lambda \mid \lambda\in\Gamma\}$.

Seja $\sigma(\eta) := \sharp M(\eta)$. *Para* $\{\ \eta_1,\eta_2,\cdots,\eta_t\ \} \subseteq \Delta(R,\rho,\varphi)$ *definimos* $\sigma(\eta_1,\eta_2,\cdots,\eta_t) := \sharp(\bigcup_{i=1}^{t} M(\eta_i))$.

(b) Para $\lambda\in\Gamma$, *definimos:*

$$N(\lambda) := \{\eta\in\Gamma \mid \exists\ \beta\in\Gamma\ com\ \eta+\beta=\lambda\}$$

Seja $\mu(\lambda) := \sharp N(\lambda)$. *Para* $\{\ \lambda_1,\cdots,\lambda_t\ \}\subseteq\Gamma$ *definimos* $\mu(\lambda_1,\cdots,\lambda_t) := \sharp\left(\bigcup_{i=1}^{t} N(\lambda_i)\right)$.

Proposição 3.1.15 *Considere o conjunto* $\Delta(R,\rho,\varphi)=\{\alpha(1),\cdots,\alpha(n)\}$ *e a base correspondente* $B=\{b_1,\cdots,b_n\}$. *Para* $i=1,\cdots,n$ *temos que* $\overline{\rho}(i)\geq\sigma(\alpha(i))$, *e para* $l=1,\cdots,n$ *temos que* $\overline{\sigma}(l)\geq\mu(\alpha(l))$. *Mais geral ainda, para* $\{a_1,\cdots,a_t\}\subseteq I$ *temos que* $\overline{\rho}(a_1,\cdots,a_t)\geq\sigma(\alpha(a_1),\cdots,\alpha(a_t))$ *e* $\overline{\mu}(a_1,\cdots,a_t)\geq\mu(\alpha(a_1),\cdots,\alpha(a_t))$.

Demonstração. Considere o conjunto $\{l \mid \alpha(l)\in M(\alpha(i))\}$. Seja $l_1\in\{l \mid \alpha(l)\in M(\alpha(i))\}$, assim existe $\alpha(j)\in\Delta(R,\rho,\varphi)$ tal que $\alpha(i)+\alpha(j)=\alpha(l_1)$, e pela proposição 3.1.12 temos que (i,j) é WB e $\overline{\rho}(b_i*b_j)=l_1$, desta forma $\{l \mid \alpha(l)\in M(\alpha(i))\}\subseteq\Lambda_i$. E como $\sharp\{l \mid \alpha(l)\in M(\alpha(i))\}=\sharp\ M(\alpha(i))=\sigma(\alpha(i))$, segue que $\overline{\sigma}(i)=\sharp(\Lambda_i\cup\{i\})\geq\sigma(\alpha(i))$.

Agora considere o conjunto $N(\alpha(l))$. Seja $\eta\in N(\alpha(l))$, logo existe $\beta\in\Gamma$ tal que $\eta+\beta=\alpha(l)$, e logo pela proposição 3.1.13 temos que existem $\alpha(i),\alpha(j)\in\Delta(R,\rho,\varphi)$ tais que $\eta=\alpha(i)$ e $\beta=\alpha(j)$. Como $\alpha(i)+\alpha(j)=\alpha(l)$, segue da proposição 3.1.12 que (i,j) é WB e $\overline{\rho}(b_i*b_j)=l$. Assim, $\{i \mid \alpha(i)\in N(\alpha(l))\}\subseteq V_l$ onde $V_l=\{i\in I \mid \overline{\rho}(b_i*b_j)=l\ para\ algum\ b_j\in B\ com\ (i,j)\ WWB\}$. Logo,

$$\overline{\mu}(l)=\sharp(V_l\cup\{l\})\geq\sharp\{i \mid \alpha(i)\in N(\alpha(l))\}=\sharp N(\alpha(l))=\mu(\alpha(l)).$$

Para a segunda parte da proposição, precisamos mostrar que:

$$\sharp\left((\Lambda_{a_1}\cup\{a_1\})\cup\cdots\cup(\Lambda_{a_t}\cup\{a_t\})\right)\geq\sharp(M(\alpha(a_1))\cup\cdots\cup M(\alpha(a_t)))$$

Note que $\sharp\left(\bigcup_{s=1}^{t} M(\alpha(a_s))\right)=\sharp\left(\bigcup_{s=1}^{t}\{l \mid \alpha(l)\in M(\alpha(a_s))\}\right)$, e pelo que fizemos acima, temos que:

$$\begin{array}{cc}\{l \mid \alpha(l)\in M(\alpha(a_1))\}\subseteq\Lambda_{a_1}\\ \{l \mid \alpha(l)\in M(\alpha(a_2))\}\subseteq\Lambda_{a_2}\\ \vdots\qquad\qquad\vdots\\ \{l \mid \alpha(l)\in M(\alpha(a_t))\}\subseteq\Lambda_{a_t}\end{array}$$

Logo, $\bigcup_{s=1}^{t}\{l \mid \alpha(l)\in M(\alpha(a_s))\}\subseteq\bigcup_{s=1}^{t}\Lambda_{a_s}\subseteq\bigcup_{s=1}^{t}(\Lambda_{a_s}\cup\{a_s\})$. E assim,

$$\sigma(\alpha(a_1),\cdots,\alpha(a_t))=\sharp\left(\bigcup_{s=1}^{t} M(\alpha(a_s))\right)=\sharp\left(\bigcup_{s=1}^{t}\{l \mid \alpha(l)\in M(\alpha(a_s))\}\right)\leq$$
$$\sharp\left(\bigcup_{s=1}^{t}(\Lambda_{a_s}\cup\{a_s\})\right)=\overline{\rho}(a_1,\cdots,a_t).$$

Agora precisamos mostrar que:

$$\sharp((V_{a_1}\cup\{a_1\})\cup\cdots\cup(V_{a_t}\cup\{a_t\}))\geq\sharp(N(\alpha(a_1))\cup\cdots\cup N(\alpha(a_t)))$$

Note que se $\eta \in N(\alpha(a_s))$ onde $s \in \{1, \cdots, t\}$, então existe $\beta \in \Gamma$ com $\eta + \beta = \alpha(a_s)$ e pela proposição 3.1.13 temos que $\eta \in \Delta(R, \rho, \varphi)$. Assim:

$$\sharp\left(\bigcup_{s=1}^{t} N(\alpha(a_s))\right) = \sharp\left(\bigcup_{s=1}^{t}\{i \mid \alpha(i) \in N(\alpha(a_s))\}\right)$$

Pelo que fizemos acima, temos que:

$$\begin{array}{c} \{i \mid \alpha(i) \in N(\alpha(a_1))\} \subseteq V_{a_1} \\ \{i \mid \alpha(i) \in N(\alpha(a_2))\} \subseteq V_{a_2} \\ \vdots \qquad\qquad \vdots \\ \{i \mid \alpha(i) \in N(\alpha(a_t))\} \subseteq V_{a_t} \end{array}$$

Assim, $\bigcup_{s=1}^{t}\{i \mid \alpha(i) \in N(\alpha(a_s))\} \subseteq \bigcup_{s=1}^{t} V_{a_s} \subseteq \bigcup_{s=1}^{t}(V_{a_s} \cup \{a_s\})$. Logo,

$$\mu(\alpha(a_1), \cdots, \alpha(a_t)) = \sharp\left(\bigcup_{s=1}^{t} N(\alpha(a_s))\right) = \sharp\left(\bigcup_{s=1}^{t}\{i \mid \alpha(i) \in N(\alpha(a_s))\}\right) \leq \sharp\left(\bigcup_{s=1}^{t}(V_{a_s} \cup \{a_s\})\right) = \overline{\mu}(a_1, \cdots, a_t).$$

como queríamos concluir. ■

Exemplo 3.1.16 *Vamos continuar o exemplo 3.1.11. Para estimar, por exemplo* $\overline{\sigma}(21)$*, temos que encontrar* $\sigma(\alpha(21))$*. Primeiro, observamos que* $\alpha(21) = 23$*. Agora veja que:*

$$M(23) = \{t \in \Delta(R, \rho, \varphi) \mid \exists\ s \in \Delta(R, \rho, \varphi) \text{ com } 23 + s = t\}$$

Logo olhamos para os valores s, t *em* $\Delta(R, \rho, \varphi)$ *tais que* $23 + s = t$*. Temos que:*

$$23 + 0 = 23,\ 23 + 3 = 26,\ 23 + 6 = 29 \text{ e } 23 + 9 = 32.$$

Assim, $M(\alpha(21)) = \{23, 26, 29, 32\}$*, e logo* $\sigma(\alpha(21)) = 4$*. Pela proposição 3.1.15 temos que* $\overline{\sigma}(21) \geq 4$*.*

Recorde que introduzimos anteriormente os códigos $\varepsilon(s)$ e os códigos melhorados $\tilde{\varepsilon}(\delta)$. Semelhantemente, introduzimos os códigos $\mathcal{C}(s)$ e os códigos melhorados $\tilde{\mathcal{C}}(\delta)$. Agora consideraremos os códigos correspondentes no contexto da teoria dos domínios de ordem.

Definição 3.1.17 *Considere o conjunto* $\Delta(R, \rho, \varphi) = \{\alpha(1), \cdots, \alpha(n)\}$ *e a base correspondente* $B = \{b_1, \cdots, b_n\}$*. Definimos*

$$\begin{array}{c} E(\lambda) := \varphi(R_\lambda) \\ = C(B, G) \text{ onde } G = \{b_i \mid \alpha(i) \preccurlyeq \lambda\} \end{array}$$

$$\begin{array}{c} \tilde{E}(\delta) := span_{\mathbb{F}_q}\{\varphi(f_{\alpha(i)}) \mid \alpha(i) \in \Delta(R, \rho, \varphi) \text{ e } \sigma(\alpha(i)) \geq \delta\} \\ = C(B, G) \text{ onde } G = \{b_i \mid \sigma(\alpha(i)) \geq \delta\} \end{array}$$

$$\begin{array}{c} C(\lambda) := \{c \in \mathbb{F}_q^n \mid c \cdot \varphi(f_\gamma) = 0 \text{ para todo } \gamma \preccurlyeq \lambda\} \\ = C^{\perp}(B, G) \text{ onde } G = \{b_i \mid \alpha(i) \preccurlyeq \lambda\} \end{array}$$

$$\begin{array}{c} \tilde{C}(\delta) := \{c \in \mathbb{F}_q^n \mid c \cdot \varphi(f_{\alpha(i)}) = 0 \text{ para todo } \alpha(i) \in \Delta(R, \rho, \varphi) \text{ com } \mu(\alpha(i)) < \delta\} \\ = C^{\perp}(B, G) \text{ onde } G = \{b_i \mid \mu(\alpha(i)) < \delta\} \end{array}$$

O seguinte teorema é uma consequência da teoria desenvolvida até agora.

Teorema 3.1.18 *A distância mínima dos códigos na definição 3.1.17 é cotada por:*

$$d(E(\lambda)) \geq min\{\sigma(\eta) \mid \eta \in \Delta(R,\rho,\varphi),\ com\ \eta \preccurlyeq \lambda\},$$

$$d(\tilde{E}(\delta)) \geq \delta,$$

$$d(C(\lambda)) \geq min\{\mu(\eta) \mid \lambda \prec \eta,\ e\ \eta \in \Delta(R,\rho,\varphi)\}$$

$$d(\tilde{C}(\delta)) \geq \delta.$$

Mais geral ainda, o t-ésimo peso generalizado de Hamming (t sendo no máximo igual a dimensão do código) satisfaz:

$$d_t(E(\lambda)) \geq min\{\sigma(\eta_1,\cdots,\eta_t) \mid \{\eta_1,\cdots,\eta_t\} \subseteq \Delta(R,\rho,\varphi)$$
$$n_i \neq n_j\ para\ i \neq j,\ \eta_s \preccurlyeq \lambda\ para\ s = 1,\cdots,t\}$$

$$d_t(\tilde{E}(\delta)) \geq min\{\sigma(\eta_1,\cdots,\eta_t) \mid \{\eta_1,\cdots,\eta_t\} \subseteq \Delta(R,\rho,\varphi)$$
$$n_i \neq n_j\ para\ i \neq j,\ \sigma(\eta_s) \geq \delta\ para\ s = 1,\cdots,t\},$$

$$d_t(C(\lambda)) \geq min\{\mu(\lambda_1,\cdots,\lambda_t) \mid \lambda_i \succ \lambda,\ \lambda_i \in \Delta(R,\rho,\varphi)$$
$$para\ i = 1,\cdots,t\}$$

$$d_t(\tilde{C}(\delta)) \geq min\{\mu(\lambda_1,\cdots,\lambda_t) \mid \mu(\lambda_i) \geq \delta,\ \lambda_i \in \Delta(R,\rho,\varphi)$$
$$para\ i = 1,\cdots,t\}$$

Demonstração. Pelo teorema 2.3.5 e proposição 3.1.15 temos que

$$d(E(\lambda)) \geq min\{\overline{\sigma}(i) \mid b_i \in G\} \geq min\{\sigma(\alpha(i)) \mid b_i \in G\}$$
$$= min\{\sigma(\eta) \mid \eta \in \Delta(R,\rho,\varphi),\ \eta \preccurlyeq \lambda\}$$

$$d(\tilde{E}(\delta)) \geq min\{\overline{\sigma}(i) \mid b_i \in G\} \geq min\{\sigma(\alpha(i)) \mid b_i \in G\} \geq \delta$$

Pelo teorema 2.4.3 e proposição 3.1.15 temos que

$$d(C(\lambda)) \geq min\{\ \overline{\mu}(l) \mid b_l \in B \setminus G\} \geq min\{\mu(\alpha(l)) \mid \alpha(l) > \lambda\}$$
$$= min\{\mu(\eta) \mid \lambda < \eta,\ \eta \in \Delta(R,\rho,\varphi)\}$$

$$d(\tilde{C}(\delta)) \geq min\{\overline{\mu}(l) \mid b_l \in B \setminus G\} \geq min\{\mu(\alpha(l)) \mid \mu(\alpha(l)) \succ \delta\} \prec \delta.$$

Pelo teorema 2.3.5 e proposição 3.1.15 segue que:

$$d_t(E(\lambda)) \geq min\{\overline{\sigma}(a_1,\cdots,a_t) \mid a_i \neq a_j\ para\ i \neq j\ e\ \{b_{a_1},\cdots,b_{a_t}\} \subseteq G\} \geq$$
$$min\{\sigma(\alpha(a_1),\cdots,\alpha(a_t)) \mid \{\alpha(a_1),\cdots,\alpha(a_s)\} \subseteq \Delta(R,\rho,\varphi),\ \alpha(a_i) \neq \alpha(a_j)\ para\ i \neq$$
$$j\ e\ \alpha(a_s) \preccurlyeq \lambda\ para\ s = 1,\cdots,t\}$$
$$= min\{\sigma(\eta_1,\cdots,\eta_t) \mid \{\eta_1,\cdots,\eta_t\} \subseteq \Delta(R,\rho,\varphi)\ \eta_i \preccurlyeq \eta_j\ para\ i \neq j,\ \eta_s \leq \lambda\ para\ s = 1,\cdots,t\}$$

$$d_t(\tilde{E}(\delta)) \geq min\{\overline{\sigma}(a_1,\cdots,a_t) \mid a_i \neq a_j\ para\ i \neq j\ \{b_{a_1},\cdots,b_{a_t}\} \subseteq G\} \geq$$
$$min\{\sigma(\alpha(a_1),\cdots,\alpha(a_t)) \mid \{\alpha(a_1),\cdots,\alpha(a_s)\} \subseteq \Delta(R,\rho,\varphi),\ \alpha(a_i) \neq \alpha(a_j)\ para\ i \neq$$
$$j\ e\ \sigma(\alpha(a_s)) \geq \delta\ para\ s = 1,\cdots,t\}$$
$$= min\{\sigma(\eta_1,\cdots,\eta_t) \mid \{\eta_1,\cdots,\eta_t\} \subseteq \Delta(R,\rho,\varphi),\ \eta_i \neq \eta_j\ para\ i \neq j,\ \sigma(\eta_s) \geq \delta\ para\ s =$$
$$1,\cdots,t\}$$

E pelo teorema 2.4.3 e proposição 3.1.15 segue que:

$$d_t(C(\lambda)) \geq min\{\overline{\mu}(a_1, \cdots, a_t) \mid a_i \neq a_j \text{ para } i \neq j \text{ e } \{b_{a_1}, \cdots, b_{a_t}\} \subseteq B \setminus G\} \geq$$
$$min\{\mu(\alpha(a_1), \cdots, \alpha(a_t)) \mid \alpha(i) \neq \alpha(a_j) \text{ para } i \neq j,\ \{\alpha(a_1), \cdots, \alpha(a_t)\} \subseteq \Delta(R, \rho, \varphi) \text{ e } \alpha(a_s) \succ$$
$$\lambda \text{ para } s = 1, \cdots, t\}$$
$$= min\{\mu(\lambda_1, \cdots, \lambda_t) \mid \lambda_i \succ \lambda,\ \lambda_i \in \Delta(R, \rho, \varphi) \text{ para } i = 1, \cdots, t\}$$

$$d_t(\tilde{C}(\delta)) \geq min\{\overline{\mu}(a_1, \cdots, a_t) \mid a_i \neq a_j \text{ para } i \neq j \text{ e } \{b_{a_1}, \cdots, b_{a_t}\} \subseteq B \setminus G\} \geq$$
$$min\{\mu(\alpha(a_1), \cdots, \alpha(a_t)) \mid \alpha(a_i) \neq \alpha(a_j) \text{ para } i \neq j,\ \{\alpha(a_1), \cdots, \alpha(a_t)\} \subseteq$$
$$\Delta(R, \rho, \varphi) \text{ e } \mu(\alpha(a_s)) \geq \delta \text{ para } s = 1, \cdots, t\}$$
$$= min\{\mu(\lambda_1, \cdots, \lambda_t) \mid \mu(\lambda_i) \geq \delta,\ \lambda_i \in \Delta(R, \rho, \varphi) \text{ para } i = 1, \cdots, t\}$$

como queríamos demonstrar. ■

É fácil ver que com relação as cotas acima a construção de $\tilde{C}(\delta)$ é um melhoramento de $C(\lambda)$ e $\tilde{E}(\delta)$ é um melhoramento de $E(\lambda)$. Os resultados sobre $d(C(\lambda))$ e $d(\tilde{C}(\delta))$ são conhecidos como a cota da ordem e são da referência [8]. Os resultados sobre $d_t(C(\lambda))$ vem da referência [9] e os resultados sobre $d_t(\tilde{C}(\delta))$ vem da referência [110]. Os resultados sobre $E(\lambda)$ e$\tilde{E}(\lambda)$ são de Andersen-Geil, referência [1].

Exemplo 3.1.19 *Isto é uma continuação do exemplo 3.1.16. Na tabela 3.3 abaixo, listamos todos os valores de* $\sigma(\alpha(i))$*, para* $i = 1, \cdots, 27$.

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\alpha(i)$	0	3	4	6	7	8	9	10	11	12	13	14	15	16
$\sigma(\alpha(i))$	27	24	23	21	20	19	18	17	16	15	14	13	12	11
i	15	16	17	18	19	20	21	22	23	24	25	26	27	
$\alpha(i)$	17	18	19	20	21	22	23	24	25	26	28	29	32	
$\sigma(\alpha(i))$	10	9	8	7	6	6	4	3	4	3	2	2	1	

Tabela 3.3: Valores de $\sigma(\alpha(i))$.

Note que $\varepsilon(21) = span_{\mathbb{F}_q}\{b_1, \cdots, b_{21}\} = E(23)$ *é um código com parâmetros* $n = 27$, $k = 21$ *e* $d \geq 4$.

E temos também que $\varepsilon(22) = span_{\mathbb{F}_q}\{b_1, \cdots, b_{22}\} = E(24)$ *é um código com parâmetros* $n = 27$, $k = 22$ *e* $d \geq 3$.

Agora veja que $\tilde{E}(4) = span_{\mathbb{F}_q}\{b_i \mid \overline{\sigma}(i) \geq 4\} = span_{\mathbb{F}_q}\{b_1, \cdots, b_{20}, b_{21}, b_{23}\}$ *é um código com parâmetros* $n = 27$, $k = 22$ *e* $d \geq 4$, *e portanto é um código melhor que os códigos* $E(23)$ *e* $E(24)$, *isto é,* $\tilde{E}(4)$ *é um código melhorado. Abaixo, segue uma tabela (tabela 3.4) com exemplos de códigos da forma* $E(\lambda)$ *e* $\tilde{E}(\delta)$ *usando-se a tabela 3.3, a cota que aparece na tabela 3.4 é a cota fornecida pelo teorema 3.1.18.*

Código	Base	Cota	Código	Base	Cota
$E(0)$	$\{b_1\}$	$d(E(0)) = 27$	$E(17)$	$\{b_1, \cdots, b_{15}\}$	$d(E(17)) \geq 10$
$E(1)$	$\{b_1\}$	$d(E(1)) = 27$	$E(18)$	$\{b_1, \cdots, b_{16}\}$	$d(E(18)) \geq 9$
$E(2)$	$\{b_1\}$	$d(E(2)) = 27$	$E(19)$	$\{b_1, \cdots, b_{17}\}$	$d(E(19)) \geq 8$
$E(3)$	$\{b_1, b_2\}$	$d(E(3)) \geq 24$	$E(20)$	$\{b_1, \cdots, b_{18}\}$	$d(E(20)) \geq 7$
$E(4)$	$\{b_1, b_2, b_3\}$	$d(E(4)) \geq 23$	$E(21)$	$\{b_1, \cdots, b_{19}\}$	$d(E(21)) \geq 6$
$E(5)$	$\{b_1, b_2, b_3\}$	$d(E(5)) \geq 23$	$E(22)$	$\{b_1, \cdots, b_{20}\}$	$d(E(22)) \geq 6$
$E(6)$	$\{b_1, \cdots, b_4\}$	$d(E(6)) \geq 21$	$E(23)$	$\{b_1, \cdots, b_{21}\}$	$d(E(23)) \geq 4$
$E(7)$	$\{b_1, \cdots, b_5\}$	$d(E(7)) \geq 20$	$E(24)$	$\{b_1, \cdots, b_{22}\}$	$d(E(22)) \geq 3$
$E(8)$	$\{b_1, \cdots, b_6\}$	$d(E(8)) \geq 19$	$E(25)$	$\{b_1, \cdots, b_{23}\}$	$d(E(25)) \geq 3$
$E(9)$	$\{b_1, \cdots, b_7\}$	$d(E(9)) \geq 18$	$E(26)$	$\{b_1, \cdots, b_{24}\}$	$d(E(26)) \geq 3$
$E(10)$	$\{b_1, \cdots, b_8\}$	$d(E(10)) \geq 17$	$E(27)$	$\{b_1, \cdots, b_{24}\}$	$d(E(27)) \geq 3$
$E(11)$	$\{b_1, \cdots, b_9\}$	$d(E(11)) \geq 16$	$E(28)$	$\{b_1, \cdots, b_{25}\}$	$d(E(28)) \geq 2$
$E(12)$	$\{b_1, \cdots, b_{10}\}$	$d(E(12)) \geq 15$	$E(29)$	$\{b_1, \cdots, b_{26}\}$	$d(E(29)) \geq 2$
$E(13)$	$\{b_1, \cdots, b_{11}\}$	$d(E(13)) \geq 14$	$E(30)$	$\{b_1, \cdots, b_{26}\}$	$d(E(30)) \geq 2$
$E(14)$	$\{b_1, \cdots, b_{12}\}$	$d(E(14)) \geq 13$	$E(31)$	$\{b_1, \cdots, b_{26}\}$	$d(E(31)) \geq 2$
$E(15)$	$\{b_1, \cdots, b_{13}\}$	$d(E(15)) \geq 12$	$E(32)$	$\{b_1, \cdots, b_{27}\}$	$d(E(32)) \geq 1$
$E(16)$	$\{b_1, \cdots, b_{14}\}$	$d(E(16)) \geq 11$			
Código	**Base**	**Cota**	**Código**	**Base**	**Cota**
$\tilde{E}(0)$	$\{b_1, \cdots, b_{27}\}$	$d(\tilde{E}(0)) \geq 0$	$\tilde{E}(15)$	$\{b_1, \cdots, b_{10}\}$	$d(\tilde{E}(15)) \geq 15$
$\tilde{E}(1)$	$\{b_1, \cdots, b_{27}\}$	$d(\tilde{E}(1)) \geq 1$	$\tilde{E}(16)$	$\{b_1, \cdots, b_9\}$	$d(\tilde{E}(15)) \geq 16$
$\tilde{E}(2)$	$\{b_1, \cdots, b_{26}\}$	$d(\tilde{E}(2)) \geq 2$	$\tilde{E}(17)$	$\{b_1, \cdots, b_8\}$	$d(\tilde{E}(17)) \geq 17$
$\tilde{E}(3)$	$\{b_1, \cdots, b_{24}\}$	$d(\tilde{E}(3)) \geq 3$	$\tilde{E}(18)$	$\{b_1, \cdots, b_7\}$	$d(\tilde{E}(18)) \geq 18$
$\tilde{E}(4)$	$\{b_1, \cdots, b_{21}, b_{23}\}$	$d(\tilde{E}(4)) \geq 4$	$\tilde{E}(19)$	$\{b_1, \cdots, b_6\}$	$d(\tilde{E}(19)) \geq 19$
$\tilde{E}(5)$	$\{b_1, \cdots, b_{20}\}$	$d(\tilde{E}(5)) \geq 5$	$\tilde{E}(20)$	$\{b_1, \cdots, b_5\}$	$d(\tilde{E}(20)) \geq 20$
$\tilde{E}(6)$	$\{b_1, \cdots, b_{20}\}$	$d(\tilde{E}(6)) \geq 6$	$\tilde{E}(21)$	$\{b_1, \cdots, b_4\}$	$d(\tilde{E}(21)) \geq 21$
$\tilde{E}(7)$	$\{b_1, \cdots, b_{18}\}$	$d(\tilde{E}(7)) \geq 7$	$\tilde{E}(22)$	$\{b_1, b_2, b_3\}$	$d(\tilde{E}(22)) \geq 22$
$\tilde{E}(8)$	$\{b_1, \cdots, b_{17}\}$	$d(\tilde{E}(8)) \geq 8$	$\tilde{E}(23)$	$\{b_1, b_2, b_3\}$	$d(\tilde{E}(23)) \geq 23$
$\tilde{E}(9)$	$\{b_1, \cdots, b_{16}\}$	$d(\tilde{E}(9)) \geq 9$	$\tilde{E}(24)$	$\{b_1, b_2\}$	$d(\tilde{E}(24)) \geq 24$
$\tilde{E}(10)$	$\{b_1, \cdots, b_{15}\}$	$d(\tilde{E}(10)) \geq 10$	$\tilde{E}(25)$	$\{b_1\}$	$d(\tilde{E}(25)) \geq 25$
$\tilde{E}(11)$	$\{b_1, \cdots, b_{14}\}$	$d(\tilde{E}(11)) \geq 11$	$\tilde{E}(26)$	$\{b_1\}$	$d(\tilde{E}(26)) \geq 26$
$\tilde{E}(12)$	$\{b_1, \cdots, b_{13}\}$	$d(\tilde{E}(12)) \geq 12$	$\tilde{E}(27)$	$\{b_1\}$	$d(\tilde{E}(27)) \geq 27$
$\tilde{E}(13)$	$\{b_1, \cdots, b_{12}\}$	$d(\tilde{E}(13)) \geq 13$			
$\tilde{E}(14)$	$\{b_1, \cdots, b_{11}\}$	$d(\tilde{E}(14)) \geq 14$			

Tabela 3.4: Exemplos de Códigos $E(\lambda)$ e $\tilde{E}(\delta)$

3.2 Códigos de Goppa de um ponto melhorados

Nesta seção, mostraremos que todo código de Goppa de um ponto pode ser visto como sendo um código da forma $E(\lambda)$ em relação a alguma estrutura de ordem, assim podemos usar os resultados da seção anterior para estimar a distância mínima.

A seguir, iremos usar alguns conceitos da teoria de corpos de funções algébricas e códigos de Goppa, o leitor que não esteja familiarizado com tais conceitos pode consultar os capítulos 1 e 2 da referência [5]. Usaremos a mesma notação da referência [5].

O seguinte exemplo é bastante conhecido:

Exemplo 3.2.1 *Seja P um lugar racional no corpo de funções $\mathbb{F}$ de uma variável com corpo de constantes $\mathbb{F}_q$. Seja v_P a valorização correspondente a P. Considere a estrutura algébrica:*

$$R = \bigcup_{m=0}^{\infty} \mathcal{L}(mP)$$

e considere a função $\rho : R \to \Gamma \cup \{-\infty\}$, definida por $\rho(f) = -v_P(f)$ onde Γ é o semigrupo de Weierstrass correspondente a P.

Vamos ver que ρ está bem definida. Seja $z \neq 0 \in R$, se Q é um pólo de z, então $Q = P$. Suponha que $v_P(z) > 0$, então $z \in P$, mas $\mathbb{F}_q \cap P = \{0\}$, logo z é transcendente sobre $\mathbb{F}_q$, assim z tem pelo menos um pólo Q. Mas Q não pode ser P pois $v_P(z) > 0$, o que é uma contradição. Portanto $v_P(z) \leq 0$. Agora sabemos que v_P é uma valorização discreta, logo tem as seguinte propriedades:

(1) $v_P(f) = \infty \Leftrightarrow f = 0$
(2) $v_P(f.g) = v_P(f) + v_P(g)$ para todo $f, g \in \mathbb{F}$
(3) $v_P(f + g) \geq min\{v_P(f), v_P(g)\}$ para todo $f, g \in \mathbb{F}$ com a igualdade ocorrendo se $v_P(f) \neq v_P(g)$.
(4) $v_P(\lambda) = 0$ para todo $\lambda \neq 0 \in \mathbb{F}_q$.
(5) Existe um elemento $z \in \mathbb{F}$ com $v_p(z) = 1$.

Desta forma ρ está de fato bem definida. E ainda mais, R é uma $\mathbb{F}_q$-álgebra e segue das propriedades (1) a (5) que ρ satisfaz as propriedades (W.0) a (W.5), logo ρ é uma função peso.

Agora sejam $P_1, \cdots, P_n$ lugares distintos de grau 1 em $\mathbb{F}$, todos eles diferentes de P, e considere a aplicação $\varphi : R \to \mathbb{F}_q^n$, definida por $\varphi(f) := (f(P_1), \cdots, f(P_n))$. Veja que se $f \in R$ então $v_{P_i}(f) \geq 0$ para $i = 1, \cdots, n$, pois $P_i \neq P$. A classe de resíduos $f(P_i)$ de f módulo P_i é um elemento do corpo de classes de resíduos de P_i, isto é, $f(P_i) \in \mathcal{O}_{P_i} / P_i$. Como $grau(P_i) = [\mathcal{O}_{P_i} / P_i : \mathbb{F}_q] = 1$, este corpo de resíduos é isomorfo a $\mathbb{F}_q$, então $f(P_i) \in \mathbb{F}_q$ e φ está bem definida.

Vamos mostrar que φ é um homomorfismo de $\mathbb{F}_q$-álgebras, para isto precisaremos do seguinte teorema cuja demonstração pode ser encontrada em [5].

***Teorema 3.2.2 (Teorema da Aproximação Forte)**. Seja $S \subsetneq \mathbb{P}_\mathbb{F}$ um subconjunto próprio de $\mathbb{P}_\mathbb{F}$ e $P_1, \cdots, P_n \in S$. Dados $g_1, \cdots, g_n \in \mathbb{F}$ e inteiros $a_1, \cdots, a_n \in \mathbb{Z}$, então existe um elemento $f \in \mathbb{F}$ tal que:*

$$v_{P_j}(f - g_j) = a_j \text{ para } (j = 1, \cdots, n), \text{ e}$$
$$v_Q(f) \geq 0 \text{ para todo } Q \in S \setminus \{P_1, \cdots, P_n\}.$$

Agora vamos mostrar que φ é sobrejetora.

Denote por $e_1 := (1, 0, \cdots, 0), e_2 := (0, 1, 0, \cdots, 0), \cdots, e_n := (0, \cdots, 0, 1) \in \mathbb{F}_q^n$. Tomando $S = \mathbb{P}_\mathbb{F} \setminus \{P\}$ e $g_1 = g_2 = \cdots = g_n = 0$ no teorema acima, temos que para cada i existe $f_i \in \mathbb{F}$ tal que:

$$v_{P_j}(f_i) = 1 \text{ para todo } j \neq i \ , \ v_{P_i}(f_i) = 0 \quad e$$
$$v_Q(f_i) \geq 0, \text{ para todo } Q \in S \setminus \{P_1, \cdots, P_n\}.$$

Veja que $S \setminus \{P_1, \cdots, P_n\} = \mathbb{P}_F \setminus \{P_1, \cdots, P_n, P\}$ *e logo* $v_Q(f_i) \geq 0$ *para todo* $Q \neq P$.

Como $v_{P_j}(f_i) = 1 > 0$ *para* $j \neq i$, *então cada* f_i *é transcendente sobre* $\mathbb{F}_q$ *e logo* f_i *tem pelo menos um pólo que nesse caso tem que ser necessariamente* P. *Logo* $v_P(f_i) < 0$.

Assim, $f_i \in R$ *e* $\varphi(f_i) = f_i(P_i)e_i$, *e temos que* $f_i(P_i) \neq 0$ *pois* $v_{P_i}(f_i) = 0 \Rightarrow f_i \in \mathcal{O}_{P_i}$ *e* $f \notin P_i$.

É fácil ver que φ *é linear e* $\varphi(fg) = \varphi(f) * \varphi(g)$ *para todo* $f, g \in R$ *e pelo que fizemos acima* φ *é sobrejetora, logo* φ *é um homomorfismo de* $\mathbb{F}_q$*-álgebras.*

Assim (R, ρ, φ) *é uma estrutura de ordem sobre* $\mathbb{F}_q$.

Observação 3.2.3 *Como* (R, ρ, φ) *é uma estrutura de ordem sobre* $\mathbb{F}_q$, *podemos considerar os subespaços* $R_\lambda = \{f \in R \mid \rho(f) \leq \lambda\}$ *de* R.

Note que se $f \in R_\lambda$, *então:*

$$\rho(f) \leq \lambda \Rightarrow -v_P(f) \leq \lambda \Rightarrow \ v_P(f) \geq -\lambda \Rightarrow f \in \mathcal{L}(\lambda P) \subseteq R.$$

Por outro lado, se $f \in \mathcal{L}(\lambda P)$, *então* $v_P(f) \geq -\lambda$ *e* $v_Q(f) \geq 0$ *para todo* $Q \neq P \in \mathbb{P}_F$ *o que nos diz que* $\rho(f) \leq \lambda$ *e* $f \in R$, *e logo* $f \in R_\lambda$. *Assim,* $R_\lambda = \mathcal{L}(\lambda P)$, *para todo* $\lambda \in \mathbb{N}_0$.

Considere a aplicação $\varphi : R \to \mathbb{F}_q^n$, *definida anteriormente por* $\varphi(f) := (f(P_1), \cdots, f(P_n))$. *Como* $P_1, \cdots, P_n$ *são lugares distintos de grau* 1 *em* $\mathbb{F}$, *todos eles diferentes de* P, *podemos considerar o código de goppa* $C_{\mathcal{L}}(P_1 + \cdots + P_n, \lambda P)$, *logo temos:*

$$\begin{aligned} C_{\mathcal{L}}(P_1 + \cdots + P_n, \lambda P) &= \{(f(P_1), \cdots, f(P_n)) \mid f \in \mathcal{L}(\lambda P)\} \\ &= \{(f(P_1), \cdots, f(P_n)) \mid f \in R_\lambda\} = \varphi(R_\lambda) = E(\lambda) \end{aligned}$$

Os códigos de Goppa da forma $C_{\mathcal{L}}(D, G)$, *onde* $G = \lambda P$ *com* $\lambda \in \mathbb{N}_0$ *e* $D = P_1 + \cdots + P_n$ *com* $P_1, \cdots, P_n$ *lugares de grau* 1 *distintos e* $P_i \neq P$ *para todo* $i = 1, \cdots, n$ *são chamados de* ***códigos de goppa de um ponto***.

Consequentemente, códigos de goppa de um ponto são códigos de goppa da forma $E(\lambda)$, *e os códigos duais dos códigos de goppa de um ponto são códigos da forma* $C(\lambda)$.

Vamos mostrar a seguir que a cota dos códigos $E(\lambda)$ no teorema 3.1.18 é um melhoramento da cota de goppa, para isto precisaremos do seguinte lema:

Lema 3.2.4 *Seja* Γ *um semigrupo numérico com um número finito de lacunas, isto é;* $\mathbb{N}_0 \setminus \Gamma$ *um conjunto finito. Então o número de elementos de* $\Gamma \setminus (i + \Gamma)$ *é igual a* i.

Demonstração. Uma demonstração deste lema pode ser encontrada na referência [4]. ■

Proposição 3.2.5 *A cota dos códigos* $E(\lambda)$ *no teorema 3.1.18 é um melhoramento da cota de Goppa.*

Demonstração. Temos que:

$$d(E(\lambda)) \geq min\{\sharp((i + \Lambda) \cap \Delta(R, \rho, \varphi)) \mid i \in \Lambda, \ i \leq \lambda\}.$$

E pelo lema anterior temos que:

$$\sharp((i+\Lambda)\cap\Delta(R,\rho,\varphi))\geq n-i$$

com igualdade se, e somente se $\Lambda\setminus(i+\Lambda)\subseteq\Delta(R,\rho,\varphi)$. De fato, temos que:

$$\Lambda=(i+\Lambda)\cup(\Lambda\setminus(i+\Lambda))$$

e essa união é disjunta. Além disso, $\Delta(R,\rho,\varphi)\subseteq(i+\Lambda)\cup(\Lambda\setminus(i+\Lambda))$. Agora se $(\Lambda\setminus(i+\Lambda))\subseteq\Delta(R,\rho,\varphi)$, então $\Delta(R,\rho,\varphi)\cap(i+\Lambda)=n-i$.

Reciprocamente, se $\Delta(R,\rho,\varphi)\cap(i+\Lambda)=n-i$, então existem i elementos de $\Delta(R,\rho,\varphi)$ que não estão em $(i+\Lambda)$, logo esses i elementos estão em $\Lambda\setminus(i+\Lambda)$, pelo lema 3.2.4 temos que $\sharp(\Lambda\setminus(i+\Lambda))=i$, segue que $\Lambda\setminus(i+\Lambda)\subseteq\Delta(R,\rho,\varphi)$. ■

A seguir, apenas para ilustração do fato de que a cota de Andersen-Geil (A-G) tem um desempenho melhor ou igual que a cota de Goppa (G), colocamos na tabela abaixo os códigos $E(\lambda)$, $\lambda=3,\cdots,30$, baseados no exemplo 3.1.11 da curva hermitiana X^4-Y^3-Y. Na tabela, k siginifica a dimensão do código $E(\lambda)$.

Código	**k**	**Cota A-G**	**Cota G**	**Código**	**k**	**Cota A-G**	**Cota G**
$E(3)$	2	24	24	$E(17)$	15	10	10
$E(4)$	3	23	23	$E(18)$	16	9	9
$E(5)$	3	23	22	$E(19)$	17	8	8
$E(6)$	4	21	21	$E(20)$	18	7	7
$E(7)$	5	20	20	$E(21)$	19	6	6
$E(8)$	6	19	19	$E(22)$	20	6	5
$E(9)$	7	18	18	$E(23)$	21	4	4
$E(10)$	8	17	17	$E(24)$	22	3	3
$E(11)$	9	16	16	$E(25)$	23	3	2
$E(12)$	10	15	15	$E(26)$	24	3	1
$E(13)$	11	14	14	$E(27)$	24	3	1
$E(14)$	12	13	13	$E(28)$	25	2	1
$E(15)$	13	12	12	$E(29)$	26	2	1
$E(16)$	14	11	11	$E(30)$	26	2	1

Tabela 3.5: Comparação entre as cotas de Andersen-Geil(A-G) e Goppa (G)

Capítulo 4

Bases de Gröbner

4.1 Uma abordagem por bases de Gröbner

Nas seções anteriores descrevemos as ferramentas necessárias para trabalharmos com códigos da teoria dos domínios de ordem; as ferramentas importantes são: a base bem ordenada $B = \{f_\lambda \mid \rho(f_\lambda) = \lambda\}_{\lambda\in\Gamma}$, o homomorfismo $\varphi : R \to \mathbb{F}_q^n$ e o conjunto $\Delta(R, \rho, \varphi)$. Lembrando que $\Delta(R, \rho, \varphi) = \{\alpha(1), \cdots, \alpha(n)\}$, onde $\alpha(1) = 0$ e $\alpha(i)$ (para $i = 2, \cdots, n$) é definido como sendo o menor elemento em Γ que é maior que $\alpha(1), \alpha(2), \cdots, \alpha(i-1)$ e satisfaz $\varphi(R_\gamma) \subsetneqq \varphi(R_{\alpha(i)})$ para todo $\gamma < \alpha(i)$. Com estas ferramentas em mãos construímos a base $B = \{b_1 = \varphi(f_{\alpha(1)}), \cdots, b_n = \varphi(f_{\alpha(n)})\}$ a qual é muito interessante para a construção de códigos.

Para um código de pequeno comprimento, normalmente encontrar o conjunto $\Delta(R, \rho, \varphi)$ é uma tarefa fácil, bastando usar somente métodos de álgebra linear básica. Contudo, para códigos de comprimentos maiores precisaremos de um método mais sofisticado. Na teoria a seguir iremos usar vários conceitos tais como: base de Gröbner, o algoritmo da divisão para polinômios em várias variáveis, e o algoritmo de Buchberger. Assumimos que o leitor tenha familiaridade com tais conceitos, e indicamos uma leitura da referência [2] para maiores detalhes.

Definição 4.1.1 *Denote por $\mathcal{M}(X_1, X_2, \cdots, X_m)$ o conjunto de todos os monômios em $X_1, X_2, \cdots, X_m$. Dada uma ordem monomial $\prec$ sobre $\mathcal{M}(X_1, X_2, \cdots, X_m)$ e um ideal $L \subseteq \mathbb{F}[X_1, \cdots, X_m]$ a **pegada de L** é o conjunto:*

$$\Delta_\prec(L) := \{M \in \mathcal{M}(X_1, X_2, \cdots, X_m) \mid M \text{ não é um monômio líder de nenhum polinômio em } L\}.$$

Observação 4.1.2 *O nome "pegada" foi sugerido por D.Blahut em 1991. A pegada foi anteriormente chamada de "delta-set", entre outros nomes.*

Somente em raros casos a pegada de um ideal L pode ser encontrada diretamente dos polinômios que definem L. Contudo, podemos sempre extender uma base qualquer de L para uma base de Gröbner de L usando o conhecido algoritmo de Buchberger , e depois podemos encontrar a pegada de L facilmente.

Definição 4.1.3 *(a) Seja $\mathbb{F}$ um corpo e seja $J \subseteq \mathbb{F}[X_1, \cdots, X_m]$ um ideal. Sejam $f, g \in \mathbb{F}[X_1, \cdots, X_m]$. Dizemos que f e g são **congruentes módulo** J, escrevendo $f \equiv g \bmod J$ se $f - g \in J$.*

*(b) Seja $\mathcal{G}$ uma base de Gröbner para J. Escreveremos **f rem $\mathcal{G}$** como o resto da divisão de f pela base $\mathcal{G}$, e vamos escrever $\overline{f}^{\mathcal{G}}$ ou simplesmente $\overline{f}$ (quando não houver risco de confusão) para denotar a classe de f em $\mathbb{F}[X_1, \cdots, X_m]/J$, onde $\overline{f} = \overline{g} \Leftrightarrow f - g \in J$.*

(c)Vamos usar a notação multi-indíce para monômios. Escreveremos $X^\alpha := \prod_{i=1}^m X_i^{\alpha_i}$ *onde* $\alpha = (\alpha_1, \cdots, \alpha_m)$.

Proposição 4.1.4 *Sejam* $\mathbb{F}$ *um corpo. Fixe uma ordem de monômios* $\prec$ *sobre* $\mathcal{M}[X_1, \cdots, X_m]$ *e seja* $I \subseteq \mathbb{F}[X_1, \cdots, X_m]$ *um ideal.*

(a) Todo $f \in \mathbb{F}[X_1, \cdots, X_m]$ *é congruente módulo* I *a um único polinômio* r *que é uma combinação* $\mathbb{F} - linear$ *de monômios em* $\Delta_\prec(I)$.

(b) Os elementos de $\Delta_\prec(I)$ *são linearmente independentes módulo* I, *isto é, se* $\sum_\alpha c_\alpha X^\alpha \equiv 0 \ mod\ I$, *onde* $X^\alpha \in \Delta_\prec(I)$ *e* $c_\alpha \in \mathbb{F}$ *para todo* α, *então* $c_\alpha = 0$ *para todo* α.

Demonstração. (a) Seja $\mathcal{G}$ uma base de Gröbner para I e seja $f \in \mathbb{F}[X_1, \cdots, X_m]$. Pelo algoritmo da divisão, o resto $r = f\ rem\ \mathcal{G}$ satisfaz $f = q + r$, onde $q \in I$. Então $f - r = q \in I$ e temos que $f \equiv r\ mod\ I$. O algoritmo da divisão também diz que r é uma combinação $\mathbb{F} - linear$ de monômios de $\Delta_\prec(I)$, e a unicidade de r segue do fato de que tomamos $\mathcal{G}$ como sendo uma base de Gröbner.

(b) Seja $\mathcal{G}$ uma base de Gröbner para I. Então se $\sum_\alpha c_\alpha X^\alpha \equiv 0\ mod\ I$ temos que $\sum_\alpha c_\alpha X^\alpha \in I$ e logo $\sum_\alpha c_\alpha c_\alpha X^\alpha rem\ \mathcal{G} = 0$. Como $X^\alpha \in \Delta_\prec(I),\ \forall \alpha$, temos que:

$$c_\alpha X^\alpha rem\ G = c_\alpha X^\alpha, \quad \forall\ \alpha$$

Consequentemente, $\sum_\alpha c_\alpha X^\alpha rem\ \mathcal{G} = \sum_\alpha c_\alpha X^\alpha$. Assim, de $\sum_\alpha c_\alpha X^\alpha rem\ \mathcal{G} = 0$, segue que $\sum_\alpha c_\alpha X^\alpha = 0$, e logo $c_\alpha = 0$, para todo α. ■

Observação 4.1.5 *Historicamente, a proposição anterior foi na verdade uma das primeiras aplicações da teoria das bases de Gröbner.*

Como consequência da proposição anterior temos o seguinte resultado:

Proposição 4.1.6 *Seja* $\mathbb{F}$ *um corpo e seja* $L \subseteq \mathbb{F}[X_1, \cdots, X_m]$ *um ideal. Então* $\{\overline{M} \mid M \in \Delta_\prec(L)\}$ *é uma base para* $\mathbb{F}[X_1, \cdots, X_m]/L$ *como espaço vetorial sobre* $\mathbb{F}$.

Uma outro resultado muito útil é a seguinte proposição que é conhecida como **Cota da Pegada**.

Proposição 4.1.7 *(a) Sejam* $\mathbb{F}$ *um corpo e* $J \subseteq \mathbb{F}[X_1, \cdots, X_m]$ *um ideal. Se* $\Delta_\prec(J)$ *é finito então* $\sharp(V_\mathbb{F}(J)) \leq \sharp(\Delta_\prec(J))$.

(b) Se $\Delta_\prec(J)$ *é finito,* J *é um ideal radical e* $\mathbb{F}$ *é algebricamente fechado, então* $\sharp(V_\mathbb{F}(J)) = \sharp(\Delta_\prec(J))$.

Demonstração. Primeiro mostraremos que dados pontos distintos $P_1, P_2, \cdots, P_r \in \mathbb{F}^m$, existe um polinômio $f_1 \in \mathbb{F}[X_1, \cdots, X_m]$ com $f_1(P_1) = 1$, e $f_1(P_2) = \cdots = f_1(P_r) = 0$. Para provar isto, observe que dados dois pontos $A = (a_1, \cdots, a_m)$, $B = (b_1, \cdots, b_m) \in \mathbb{F}^m$ com $A \neq B$, então eles diferem em pelo menos uma coordenada, digamos a j-ésima, e assim tomando $g = \dfrac{X_j - b_j}{a_j - b_j}$ temos que g satisfaz $g(A) = 1$ e $g(B) = 0$. Aplicando esta observação para cada par P_1, P_i com $P_1 \neq P_i,\ i \geq 2$, obtemos polinômios $g_{i's}$ tais que $g_i(P_1) = 1$ e $g_i(P_i) = 0$ para $i \geq 2$. Então $f_1 = g_2.g_3 \cdots g_r$ tem a propriedade desejada.

Neste argumento que acabamos de dar, não existe nada em especial com P_1. Se aplicarmos o mesmo argumento com cada P_i, $i \geq 1$, teremos polinômios $f_1, \cdots, f_r$ tais que $f_i(P_i) = 1$ e $f_i(P_j) = 0$ para $i \neq j$. Agora, podemos provar o teorema.

(a) Seja $\mathcal{G}$ uma base de Gröbner e seja $V := \{P_1, \cdots, P_r\} \subseteq \mathbb{V}_{\mathbb{F}}(J)$, onde os $P_{i's}$ são todos distintos. Então temos $f_1, \cdots, f_r$ como acima, isto é; $f_i(P_i) = 1$ *e* $f_i(P_j) = 0$ *para* $i \neq j$. Seja $\sum_{i=1}^{r}(a_i f_i \; rem \; \mathcal{G}) = 0$ uma combinação linear em $\mathbb{F}[X_1, \cdots, X_m]/J$, onde $a_i \in \mathbb{F}$. Voltando em $\mathbb{F}[X_1, \cdots, X_m]$, como $\sum_{i=1}^{r}(a_i f_i \; rem \; \mathcal{G}) = 0$, então $h := \sum_{i=1}^{r} a_i f_i \in J$, e como $\mathbb{V}_{\mathbb{F}}(J) = \{P \in \mathbb{F}^m \mid f(P) = 0 \; \forall f \in J\}$, segue que h se anula em todos os pontos de $\mathbb{V}_{\mathbb{F}}(J)$, em particular; h se anula em $V \subseteq \mathbb{V}_{\mathbb{F}}(J)$. Então, para $1 \leq j \leq r$, temos:

$$0 = h(P_j) = \sum_{i=1}^{r} a_i f_i(P_j) = a_j f_j(P_j) = a_j$$

e temos que $f_1 \; rem \; \mathcal{G}, \cdots, f_r \; rem \; \mathcal{G}$ são r elementos linearmente independentes em $\mathbb{F}[X_1, \cdots, X_m]/J$.

Assim, para cada r pontos em $\mathbb{V}_{\mathbb{F}}(J)$ existem r elementos linearmente independentes em $\mathbb{F}[X_1, \cdots, X_m]/J$. Agora, $\Delta_{\prec}(J)$ forma uma base para $\mathbb{F}[X_1, \cdots, X_m]/J$ como espaço vetorial, e $\Delta_{\prec}(J)$ é finito; seja $s := \sharp(\Delta_{\prec}(J))$, assim pelo que fizemos acima existem no máximo s pontos distintos em $\mathbb{V}_{\mathbb{F}}(J)$, e segue o que queríamos provar.

(b)Suponha que J é radical. Para mostrarmos que $\sharp(V_{\mathbb{F}}(J)) = \sharp(\Delta_{\prec}(J))$ basta mostrarmos que $B = \{f_1 \; rem\mathcal{G}, \cdots, f_r \; rem\mathcal{G}\}$ é uma base para $\mathbb{F}[X_1, \cdots, X_m]/J$. No item (a) já provamos a independência linear, precisamos então mostrar apenas que B gera $\mathbb{F}[X_1, \cdots, X_m]/J$. Seja $\overline{g} \in \mathbb{F}[X_1, \cdots, X_m]/J$, e denote $a_i := g(P_i)$ e considere $h := g - \sum_{i=1}^{r} a_i f_i$. Note que $h(P_j) = 0$ para todo j, assim $h \in I(V(J)) = \{f \in \mathbb{F}[X_1, \cdots, X_m] \mid f(P) = 0 \; \forall P \in V(J)\}$.
Agora temos que $\mathbb{F}$ é algebricamente fechado e J é radical, logo pelo teorema (forte) de zeros de Hilbert, $I(V(J)) = \sqrt{J} = J$, e assim $h \in J$. Logo $\overline{h} = \overline{0}$ em $\mathbb{F}[X_1, \cdots, X_m]/J$, o que implica que $\overline{g} = \sum_{i=1}^{r} a_i \overline{f_i}$. ■

Agora vamos introduzir as ordens que serão importantes para nós. Elas são as **ordens grau com pesos generalizadas**.

Definição 4.1.8 *Dados pesos* $w(X_1), \cdots, w(X_m) \in \mathbb{N}_0^r \; \{0\}$, *seja* $\mathbb{N}_0^r$ *ordenado por alguma ordem monomial* $\prec_{\mathbb{N}_0^r}$ *fixada e seja* $\prec_{\mathcal{M}}$ *uma ordem monomial fixada sobre* $\mathcal{M}(X_1, \cdots, X_m)$. *Os pesos se extendem para um monômio pela função* $w : \mathcal{M}(X_1, \cdots, X_m) \to \mathbb{N}_0^r$ *definida por* $w(X_1^{\alpha_1}.X_2^{\alpha_2} \cdots X_m^{\alpha_m}) = \sum_{i=1}^{m} \alpha_i w(X_i)$. *Para um monômio* M *dizemos que* $w(M)$ *é o* ***peso de*** M. *Definimos o* ***grau com pesos*** $wdeg(F)$ *de um polinômio* F *como sendo o maior peso (com relação a* $\prec_{\mathbb{N}_0^r}$*) que aparece como peso de um monômio no suporte de* F. *Agora, a ordem* ***grau com pesos generalizada*** $\prec_w$ *induzida por* w, $\prec_{\mathbb{N}_0^r}$ *e* $\prec_{\mathcal{M}}$ *é a ordem monomial definida a seguir. Dados* $M_1, M_2 \in \mathcal{M}(X_1, \cdots, X_m)$, *então* $M_1 \prec_w M_2$ *se e somente se uma das duas seguintes condições ocorrem:*

$$(1) \; w(M_1) \prec_{\mathbb{N}_0^r} w(M_2), \qquad (2) \;\; w(M_1) = w(M_2) \; e \; M_1 \prec_{\mathcal{M}} M_2.$$

Estamos agora em condições de dar uma descrição útil para os domínios de ordem finitamente gerados.

Teorema 4.1.9 *Seja* $\prec_w$ *uma ordem grau com pesos generalizada e assuma que* $I \subseteq \mathbb{F}[X_1, \cdots, X_m]$ *é um ideal com uma base de Gröbner* $\mathcal{G}$ *com relação a* $\prec_w$. *Suponha que os elementos da pegada* $\Delta_{\prec_w}(I)$ *tem distintos pesos e que todo elemento de* $\mathcal{G}$ *tem exatamente dois monômios de maior peso (com relação a* $\prec_{\mathbb{N}_0^r}$*) em seu suporte. Então* $R =$

$\mathbb{F}[X_1, \cdots, X_m]/I$ é um domínio de ordem com uma função peso definida a seguir: Dado um $f \neq 0 \in \mathbb{F}[X_1, \cdots, X_m]/I$ escreva $f = F + I$ onde $F \in span_{\mathbb{F}}\{M \mid M \in \Delta_{\prec_w}(I)\}$. Temos que $\rho(f) = wdeg(F)$ e $\rho(0) = -\infty$. E ainda mais, qualquer domínio de ordem finitamente gerado pode ser descrito desta forma.

Demonstração. A demonstração deste teorema pode ser encontrada na referência [3, teoremas 9.1 e 10.4]. ■

Exemplo 4.1.10 *Neste exemplo mostramos como o domínio de ordem e a função peso descrita no exemplo 3.1.16 podem ser facilmente explicados pelo teorema 4.1.9. Os pesos das variáveis são $w(X) = 3$ e $w(Y) = 4$, a ordem monomial $\prec_{\mathbb{N}_0}$ é a usual (que é a única ordem monomial sobre $\mathbb{N}_0$ e a ordem $\prec_{\mathcal{M}}$ sobre $\mathcal{M}(X, Y)$ é a ordem lexicográfica com $X \prec_{\mathcal{M}} Y$. A ordem grau com pesos generalizada $\prec_w$ resultante nos dá a seguinte pegada:*

$$\Delta_{\prec_w}(I) = \{X^\alpha Y^\beta \mid 0 \leq \alpha,\ 0 \leq \beta < 3\}$$

Apenas para ilustração, podemos fazer uma correspondência dos pontos em $\mathbb{N}_0^2$ com os monômios em $\mathcal{M}(X, Y)$ da seguinte maneira: a cada ponto $(m, n) \in \mathbb{N}_0^2$ associamos o monômio $X^m Y^n \in \mathcal{M}(X, Y)$ e vice-versa. Desta forma a pegada acima pode ser representada como os pontos que não estão na faixa (infinita) hachurada na figura abaixo.

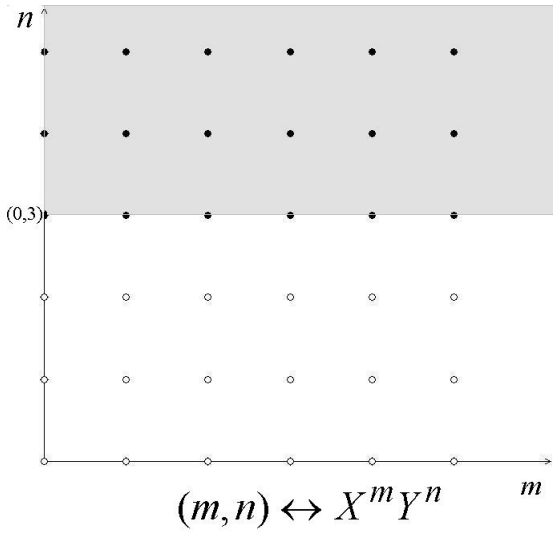

Figura 4.1: A pegada $\Delta_{\prec_w}(I)$

É fácil ver que a aplicação $w : \Delta_{\prec_w}(I) \to \langle 3, 4\rangle$ dada por $w(X^i Y^j) = 3i + 4j$ é uma bijeção. Logo, os elementos de $\Delta_{\prec_w}(I)$ tem pesos distintos. Note que $G = \{X^4 - Y^3 - Y\}$ é uma base de Gröbner para I, e que $w(Y^3) = w(X^4) = 12$, isto é; $X^4 - Y^3 - Y$ tem dois monômios de maior grau. Assim, a pegada $\Delta_{\prec_w}(I)$ satisfaz as condições do teorema 4.1.9, e note que a função peso dada no teorema 4.1.9 é exatamente a mesma descrita no exemplo 3.1.16. A base bem comportada do exemplo 3.1.16 é encontrada usando-se a proposição 4.1.6 sobre a pegada acima.

Agora, precisamos escolher um homomorfismo $\varphi : R \to \mathbb{F}_q^n$ sobre o domínio de ordem $R = \mathbb{F}_q[X_1, \cdots, X_m]/I$. A escolha mais óbvia de homomorfismo é a aplicação de avaliação sobre a variedade afim $\mathbb{V}_{\mathbb{F}_q}(I) = \{P_1, \cdots, P_n\}$. Em outras palavras, o homomorfismo $\varphi : R \to \mathbb{F}_q^n$ dado por $\varphi(F + I) := (F(P_1), \cdots, F(P_n))$.

Uma pergunta natural neste momento seria: o que acontece se escolhermos um outro homomorfismo $\tilde{\varphi} : R \to \mathbb{F}_q^n$ sobre o domínio de ordem $R = \mathbb{F}_q[X_1, \cdots, X_m]/I$, que não seja a aplicação de avaliação φ?

O próximo resultado nos ajudará a responder esta pergunta.

Teorema 4.1.11 *Seja $\varphi : \mathbb{F}_q[X_1, \cdots, X_m]/I \to \mathbb{F}_q^n$ uma aplicação sobrejetora $\mathbb{F}_q$-linear satisfazendo $\varphi(fg) = \varphi(f) * \varphi(g)$ para todo $f, g \in \mathbb{F}_q[X_1, \cdots, X_m]/I$. Então existe um conjunto $\{P_1, \cdots, P_n\} \subseteq V_{\mathbb{F}_q}(I)$, $P_i \neq P_j$ para $i \neq j$ tal que $\varphi(F(X_1, \cdots, X_m)+I) = (F(P_1), \cdots, F(P_n))$ ocorre para todo $F(X_1, \cdots, X_m) \in \mathbb{F}_q[X_1, \cdots, X_m]$.*

Demonstração. Seja $\pi_i : \mathbb{F}_q^n \to \mathbb{F}_q$ a aplicação de projeção na i-ésima coordenada, isto é; $\pi_i(a_1, a_2, \cdots, a_n) = a_i$. Como φ é uma aplicação $\mathbb{F}_q$-linear sobrejetora, então para cada $i = 1, \cdots, n$ a aplicação $\varphi_i : \mathbb{F}_q[X_1, \cdots, X_m]/I \to \mathbb{F}_q$ definida por $\varphi_i(F + I) = \pi_i(\varphi(F + I))$ é $\mathbb{F}_q$-linear e sobrejetora, além disso essas aplicações são todas distintas.

Seja $a = (a_1, a_2, \cdots, a_n) \in \mathbb{F}_q^n$ tal que $\varphi(1 + I) = a$, e sejam $b = (b_1, b_2, \cdots, b_n) \in \mathbb{F}_q^n$ com $b_i \neq 0$ para todo $i = 1, \cdots, n$ e $F + I \in \mathbb{F}_q[X_1, \cdots, X_m]/I$ tal que $\varphi(F + I) = b$. Veja que $\varphi(F + I) = \varphi((1 + I)(F + I)) = \varphi(1 + I) * \varphi(F + I) = (a_1b_1, \cdots, a_nb_n) = (b_1, \cdots, b_n)$, assim $\varphi(1+I) = (1, 1, \cdots, 1)$, e logo φ é um homomorfismo de anéis. E como φ é $\mathbb{F}_q$-linear segue que $\varphi(c+I) = (c, c, \cdots, c)$ para todo $c \in \mathbb{F}_q$. Assim, cada φ_i é um homomorfismo com $\varphi_i(c+I) = c$ para todo $c \in \mathbb{F}_q$. Sejam

$$\begin{array}{c} P_1 = (P_1^{(1)}, P_1^{(2)}, \cdots, P_1^{(m)}) \in \mathbb{F}_q^m \\ P_2 = (P_2^{(1)}, P_2^{(2)}, \cdots, P_2^{(m)}) \in \mathbb{F}_q^m \\ \vdots \quad \vdots \quad \vdots \\ P_n = (P_n^{(1)}, P_n^{(2)}, \cdots, P_n^{(m)}) \in \mathbb{F}_q^m \end{array}$$

tais que

$$\begin{array}{c} P_1^{(1)} = \varphi_1(X_1 + I), P_1^{(2)} = \varphi_1(X_2 + I), \cdots, P_1^{(m)} = \varphi_1(X_m + I) \\ P_2^{(1)} = \varphi_2(X_1 + I), P_2^{(2)} = \varphi_2(X_2 + I), \cdots, P_2^{(m)} = \varphi_2(X_m + I) \\ \vdots \quad \vdots \quad \vdots \\ P_i^{(1)} = \varphi_i(X_1 + I), P_i^{(2)} = \varphi_i(X_2 + I), \cdots, P_i^{(m)} = \varphi_i(X_m + I) \\ \vdots \quad \vdots \quad \vdots \\ P_n^{(1)} = \varphi_n(X_1 + I), P_n^{(2)} = \varphi_n(X_2 + I), \cdots, P_n^{(m)} = \varphi_n(X_m + I) \end{array}$$

Seja $<$ uma ordem monomial sobre o conjunto de todos os monômios em $X_1, \cdots, X_m$. Temos que o conjunto $\{M + I \mid M \in \Delta_<(I)\}$ é uma base para $\mathbb{F}_q[X_1, \cdots, X_m]/I$ como $\mathbb{F}_q$-espaço vetorial, seja $M = X_1^{\alpha_1}X_2^{\alpha_2} \cdots X_m^{\alpha_m} \in \Delta_<(I)$, e seja $G = cM$, onde $c \in \mathbb{F}_q$, logo temos que

$$G(P_i) = G((P_i^{(1)}, P_i^{(2)}, \cdots, P_i^{(m)})) = c(P_i^{(1)})^{\alpha_1}(P_i^{(2)})^{\alpha_2} \cdots (P_i^{(m)})^{\alpha_m} =$$
$$\varphi_i(c + I)\varphi_i(X_1^{\alpha_1} + I)\varphi_i(X_2^{\alpha_2} + I) \cdots \varphi_i(X_m^{\alpha_m} + I) = \varphi_i(cX_1^{\alpha_1}X_2^{\alpha_2} \cdots X_m^{\alpha_m} + I) = \varphi_i(cM + I).$$

Assim, $\varphi_i(cM + I) = cM(P_i)$ para todo $M \in \Delta_<(I)$, $c \in \mathbb{F}_q$ *e* $i = 1, \cdots, n$. Como qualquer $f \in \mathbb{F}_q[X_1, \cdots, X_m]/I$ pode ser escrito como $f = F + I$ onde $F \in span_{\mathbb{F}_q}\{M \mid M \in \Delta_<(I)\}$ e φ_i é $\mathbb{F}_q$-linear, segue que $\varphi_i(F + I) = F(P_i)$ para todo $i = 1, \cdots, n$.

Assim, $\varphi(F + I) = (F(P_1), F(P_2), \cdots, F(P_n))$. Agora, vamos mostrar que $P_i \in \mathbb{V}_{\mathbb{F}_q}(I)$ para todo $i = 1, \cdots, n$. Para todo $H(X_1, \cdots, X_m) \in I$ temos que

$$\varphi(H(X_1,\cdots,X_m)+I)=\varphi(0+I)=(0,0,\cdots,0)=(H(P_1),\cdots,H(P_n)).$$

Logo $H(P_1)=H(P_2)=\cdots=H(P_n)=0$ para todo $H\in I$, assim $P_1,P_2,\cdots,P_n\in\mathbb{V}_{\mathbb{F}_q}(I)$. ■

Definição 4.1.12 *Dado um ideal $I\subseteq\mathbb{F}_q[X_1,\cdots,X_m]$ escrevemos*

$$I_q:=I+\langle X_1^q-X_1,X_2^q-X_2,\cdots,X_m^q-X_m\rangle.$$

Observação 4.1.13 *Sejam $\mathbb{F}=\mathbb{F}_q$, $I_q\subseteq\mathbb{F}_q[X_1,\cdots,X_m]$ como na definição acima, e seja $\prec$ uma ordem sobre $\mathcal{M}(X_1,\cdots,X_m)$. Então $\sharp(\mathbb{V}_{\mathbb{F}_q}(I_q))=\sharp(\Delta_\prec(I_q))$.*

Proposição 4.1.14 *Considere uma estrutura de ordem (R,ρ,Γ) como descrita no teorema 4.1.9. Seja φ o homomorfismo $\varphi:R\to\mathbb{F}_q^n$ dado por $\varphi(F+I):=(F(P_1),F(P_2),\cdots,F(P_n))$ onde $V_{\mathbb{F}_q}(I)=\{P_1,\cdots,P_n\}$. Temos que*

$$\Delta(R,\rho,\varphi)=\{\ w(M)\mid M\in\Delta_{\prec_w}(I_q)\ \}$$

Demonstração. Uma das condiçoes no teorema 4.1.9 e que os pesos dos monomios em $\Delta_{\prec_w}(I)$ sejam todos distintos. Como $I\subseteq I_q$, logo $\Delta_{\prec_w}(I_q)\subseteq\Delta_{\prec_w}(I)$ e os pesos de todos os monômios em $\Delta_{\prec_w}(I_q)$ também são todos distintos. Consequentemente, o número de elementos de $\{w(M)\mid M\in\Delta_{\prec_w}(I_q)\}$ é igual ao número de elementos de $\Delta_{\prec_w}(I_q)$. Mas pela observação 4.1.13 temos que $\sharp(\Delta_{\prec_w}(I_q)=\sharp(\mathbb{V}_{\mathbb{F}_q}(I_q))=\sharp(\mathbb{V}_{\mathbb{F}_q}(I))$, logo $\sharp(\{w(M)\mid M\in\Delta_{\prec_w}(I_q)\})=n$. E ainda temos que $\sharp(\Delta(R,\rho,\varphi)=n$, pois φ é sobrejetora. Assim,

$$\sharp(\Delta(R,\rho,\varphi))=\sharp(\{w(M)\mid M\in\Delta_{\prec_w}(I_q)\})$$

A proposiçao portanto estara provada se mostrarmos que $\alpha(s)\in\{w(M)\mid M\in\Delta_{\prec_w}(I_q)\}$ para $s=1,2,\cdots,n$. Fixe $\alpha(s)\in\Delta(R,\rho,\Gamma)$ e seja $f\in R$ tal que $\rho(f)=\alpha(s)$. Pela construção do teorema 4.1.9 podemos escrever $f=F+I$ onde $F=\sum_{i=1}^t\eta_iM_i$, $t\geq1$, $M_i\in\Delta_{\prec_w}(I)$, $\eta_i\in\mathbb{F}_q\setminus\{0\}$ para $i=1,2,\cdots,t$, $w(M_t)\prec_{\mathbb{N}_0^r}w(M_{t-1})\prec_{\mathbb{N}_0^r}\cdots\prec_{\mathbb{N}_0^r}w(M_1)$, e onde $\alpha(s)=\rho(f)=wdeg(F)=w(M_1)$.

Seja G' uma base de Gröbner para I_q com relação a $\prec_w$. Agora, reduzindo F módulo G' usando o algoritmo da divisão para polinômios, obtemos um resto $\sum_{i=1}^l\beta_iN_i$ (que vamos mostrar ser diferente de zero) onde $N_i\in\Delta_{\prec_w}(I_q)$, $\beta_i\in\mathbb{F}_q\setminus\{0\}$ *para* $i=1,2,\cdots,l$ e onde $w(N_l)\prec_{\mathbb{N}_0^r}w(N_{l-1})\prec_{\mathbb{N}_0^r}\cdots\prec_{\mathbb{N}_0^r}w(N_1)$. Temos que $F-\sum_i^l\beta_iN_i\in I_q$ e como $\mathbb{V}_{\mathbb{F}_q}(I_q)=\mathbb{V}_{\mathbb{F}_q}(I)=\{P_1,\cdots,P_n\}$, então $\varphi(F-\sum_{i=1}^l\beta_iN_i+I)=0$. Logo,

$$\varphi(f)=\varphi(F+I)=\varphi(F+I)-\varphi(F-\sum_{i=1}^l\beta_iN_i+I)= \tag{4.1}$$

$$=\varphi(F-(F-\sum_{i=1}^l\beta_iN_i)+I)=\varphi(\sum_{i=1}^l\beta_iN_i+I) \tag{4.2}$$

Note que pela definição de $\alpha(s)$ temos que $\varphi(f)\neq0$. Portanto, por 4.2 temos que $\sum_{i=1}^l\beta_iN_i\neq0$. Este fato e o fato de que $\Delta_{\prec_w}(I_q)\subseteq\Delta_{\prec_w}(I)$ implicam que:

$$\rho(\textstyle\sum_{i=1}^l\beta_iN_i+I)=w(N_1).$$

Agora, observe que pela natureza do algoritmo da divisão e pela definição de $\prec_w$, temos que $wdeg(F)\succeq_{\mathbb{N}_0^r}wdeg(\sum_{i=1}^l\beta_iN_i)$. Isto é o mesmo que dizer que:

$$\alpha(s) = \rho(f) = wdeg(F) = w(M_1) \succeq_{\mathbb{N}_0^r} w(N_1) = wdeg(\sum_{i=1}^{l} \beta_i N_i) = \rho(\sum_{i=1}^{l} \beta_i N_i + I).$$

Pela definição de $\Delta(R, \rho, \varphi)$, temos que $\varphi(R_\lambda) \subsetneqq \varphi(R_{\alpha(s)})$ para todo $\lambda \prec_{\mathbb{N}_0^r} \alpha(s)$. Em particular, isto implica que $\varphi(g) \neq \varphi(f)$ para todo $g \in R$ com $\rho(g) \prec_{\mathbb{N}_0^r} \rho(f)$. Suponha que $w(N_1) \prec_{\mathbb{N}_0^r} \rho(f)$, como $\rho(\sum_{i=1}^{l} \beta_i N_i + I) = w(N_1)$, então $\varphi(\sum_{i=1}^{l} \beta_i^l \beta_i N_i + I) \neq \varphi(f)$. Uma contradição. Logo, $\alpha(s) = w(N_1) \in \Delta_{\prec_w}(I_q)$ e segue que a proposição está provada. ■

Exemplo 4.1.15 *Isto é uma continuação do exemplo 4.1.10. Podemos mostrar que:*

$$\Delta_{\prec_w}(I_q) = \{X^\alpha Y^\beta \mid 0 \leq \alpha < 9,\ 0 \leq \beta < 3\}$$

Consequentemente, temos que $\Delta(R, \rho, \varphi) = \{X^\alpha Y^\beta \mid 0 \leq \alpha < 9,\ 0 \leq \beta < 3\}$ *que por inspeção, nos fornece exatamente a base B encontrada no exemplo 3.1.11.*

Esta pegada é particulamente simples no sentido em que dizemos que ela tem o formato de uma "caixa". Por inspeção, temos como uma consequência deste fato o seguinte:

$$\mu(\rho(X^\alpha Y^\beta + I)) = \sigma(\rho(X^{8-\alpha} Y^{2-\beta} + I))$$

para todo α, β *com* $X^\alpha Y^\beta$ *na pegada de* I_q.

Como exemplo podemos citar:

$$\rho(X^5 Y + I) = 19 \quad e \quad \rho(X^{8-5} Y^{2-1} + I) = 13$$

Logo,

$$\mu(19) = \sharp(N(19)) = \sharp(\{\eta \in \Gamma \mid \exists \beta \in \Gamma \ com\ \eta + \beta = 19\}) = \sharp(\{0, 3, 4, 6, 7, 8, 9, 10, 11, 12, 13, 15, 16, 19\}) = 14$$

$$\sigma(13) = \sharp(M(13)) = \sharp(\{\gamma \in \Delta(R, \rho, \varphi) \mid \exists \beta \in \Delta(R, \rho, \varphi)\ com\ 13 + \beta = \gamma\}) = = \sharp(\{13, 16, 17, 19, 20, 21, 22, 23, 24, 25, 26, 28, 29, 32\}) = 14$$

Portanto, em particular a cota de Feng-Rao nos fornece a mesma estimativa para a distância mínima do código $c(\alpha(s))$ *que a cota de Andersen-Geil fornece para o código* $E(\alpha(n-s))$, $s = 1, \cdots, n-1$.

Podemos provar este fato no seguinte resultado:

Proposição 4.1.16 *: Seja R um domínio de ordem sobre* $\mathbb{F}_q$ *descrito como no teorema 4.1.9. Seja* $\mathbb{V}_{\mathbb{F}_q}(I_q) = \{P_1, \cdots, P_n\}$ *e considere a aplicação de avaliação* $\varphi : R \to \mathbb{F}_q^n$ *dada por* $\varphi(F + I) = (F(P_1), \cdots, F(P_n))$. *Seja* $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \cdots, \alpha(n)\}$ *definido como anteriormente. Se* $\Delta_{\prec_w}(I_q)$ *é da forma:*

$$\Delta_{\prec_w}(I_q) = \{X_1^{\beta_1} X_2^{\beta_2} \cdots X_m^{\beta_m} \mid \beta_1 \leq \gamma_1, \beta_2 \leq \gamma_2, \cdots, \beta_m \leq \gamma_m\}$$

para algum $(\gamma_1, \gamma_2, \cdots, \gamma_m) \in \mathbb{N}^m$*, então:*

(a) $\mu(\rho(X_1^{\beta_1} \cdots X_m^{\beta_m} + I)) = \sigma(\rho(X_1^{\gamma_1-\beta_1} \cdots X_m^{\gamma_m-\beta_m} + I))$*, ocorre para qualquer* $X_1^{\beta_1} \cdots X_m^{\beta_m} \in \Delta_{\prec_w}(I_q)$*.*
(b) $\alpha(n) - \alpha(l) = \alpha(n - l + 1)$*, para todo* $l = 1, \cdots, n$*.*
(c) Para qualquer s *com* $1 \leq s < n$*, os códigos* $C(\alpha(s))$ *e* $E(\alpha(n-s))$ *são de mesma dimensão.*
(d) Para qualquer s *com* $1 \leq s < n$*, a cota de Feng-Rao fornece exatamente as mesmas estimativas para o t-ésimo peso generalizado de Hamming de* $C(\alpha(s))$ *que a cota de Andersen-Geil fornece para o t-ésimo peso generalizado de Hamming de* $E(\alpha(n - s))$*.*
(e) Para qualquer δ *a dimensão de* $\tilde{C}(\delta)$ *é igual a dimensão de* $\tilde{E}(\delta)$*.*
(f) Para qualquer t *(no máximo igual a dimensão de* $\tilde{C}(\delta)$*), a cota de Feng-Rao fornece exatamente as mesmas estimativas sobre o t-ésimo peso generalizado de Hamming de* $\tilde{C}(\delta)$ *que a cota de Andersen-Geil fornece para o t-ésimo peso generalizado de Hamming de* $\tilde{E}(\delta)$*.*

Demonstração. (a) Seja $\alpha(l) \in \Delta(R, \rho, \varphi) = \{w(M) \mid M \in \Delta_{\prec_w}(I_q)\}$. Por hipótese, existem $w_1, w_2, \cdots, w_m \in \mathbb{N}_0$ com $w_1 \leq \gamma_1, w_2 \leq \gamma_2, \cdots, w_m \leq \gamma_m$ tais que $w(X_1^{w_1} X_2^{w_2} \cdots X_m^{w_m}) = \alpha(l)$. Também por hipótese temos que:

$$w(X_1^{\gamma_1-w_1} X_2^{\gamma_2-w_2} \cdots X_m^{\gamma_m-w_m}) \in \Delta(R, \rho, \varphi).$$

Consequentemente, se escrevermos $\alpha_{max} := w(X_1^{\gamma_1} X_2^{\gamma_2} \cdots X_m^{\gamma_m})$ então temos que:

$$\alpha(l) \in \Delta(R, \rho, \varphi) \Leftrightarrow \alpha_{max} - \alpha(l) \in \Delta(R, \rho, \varphi).$$

Note que $\mu(\alpha(l)) = \sigma(\alpha_{max} - \alpha(l))$. De fato, veja que:

$$\mu(\alpha(l)) = \sharp(N(\alpha(l)) = \sharp\{\eta \in \Gamma \mid \exists \beta \in \Gamma \text{ com } \eta + \beta = \alpha(l)\} =$$
$$\sharp\{\eta \in \Delta(R, \rho, \varphi) \mid \exists \beta \in \Delta(R, \rho, \varphi) \text{ com } \eta + \beta = \alpha(l)\} \text{ e}$$
$$\sigma(\alpha_{max} - \alpha(l)) = \sharp(M(\alpha_{max} - \alpha(l))) =$$
$$\sharp\{\gamma \in \Delta(R, \rho, \varphi) \mid \exists \theta \in \Delta(R, \rho, \varphi) \text{ com } (\alpha_{max} - \alpha(l)) + \theta = \gamma\}$$

Defina $g : N(\alpha(l)) \to M(\alpha_{max} - \alpha(l))$ por $g(\eta) = \alpha_{max} - \eta$. Veja que g está bem definida pois se $\eta \in N(\alpha(l))$ logo $\eta \in \Delta(R, \rho, \varphi)$ (e logo $\alpha_{max} - \eta \in \Delta(R, \rho, \varphi)$) e existe $\beta \in \Delta(R, \rho, \varphi)$ com

$$\eta + \beta = \alpha(l) \tag{4.3}$$

De 4.3 segue que $(\alpha_{max} - \alpha(l)) + \beta = \alpha_{max} - \eta$, e portanto $\alpha_{max} - \eta \in M(\alpha_{max} - \alpha(l))$. Temos que g é injetora, agora seja $\gamma \in M(\alpha_{max} - \alpha(l))$, então $\gamma \in \Delta(R, \rho, \varphi)$ (e logo $\alpha_{max} - \gamma \in \Delta(R, \rho, \varphi)$) e existe $\theta \in \Delta(R, \rho, \varphi)$ tal que

$$(\alpha_{max} - \alpha(l)) + \theta = \gamma \tag{4.4}$$

De 4.4 segue que $(\alpha_{max} - \gamma) + \theta = \alpha(l)$, e logo $\alpha_{max} - \gamma \in N(\alpha(l))$, e ainda temos que $g(\alpha_{max} - \gamma) = \gamma$, logo g é sobrejetora. Portanto, $\mu(\alpha(l)) = \sigma(\alpha_{max} - \alpha(l))$ e logo

$$\mu(\rho(X_1^{\beta_1} \cdots X_m^{\beta_m} + I)) = \sigma(\rho(X_1^{\gamma_1-\beta_1} \cdots X_m^{\gamma_m-\beta_m} + I)) \tag{4.5}$$

para qualquer $X_1^{\beta_1} \cdots X_m^{\beta_m} \in \Delta_{\prec_w}(I_q)$.

(b) Para cada $\alpha(s) \in \Delta(R, \rho, \varphi)$ temos por hipótese que $\alpha(n) - \alpha(s) \in \Delta(R, \rho, \varphi)$. Sejam $\alpha(l_1), \alpha(l_2) \in \Delta(R, \rho, \varphi)$ como $\alpha(n) - \alpha(l_1) = \alpha(n) - \alpha(l_2)$ se, e somente se $\alpha(l_1) = \alpha(l_2)$, então para cada $\alpha(s) \in \Delta(R, \rho, \varphi)$ existe um único $\alpha(l) \in \Delta(R, \rho, \varphi)$ tal que $\alpha(n) - \alpha(l) = \alpha(s)$. Temos que $\alpha(n) - \alpha(1) = \alpha(n - 1 + 1) = \alpha(n)$. Suponha que $\alpha(n) - \alpha(2) \neq \alpha(n - 1)$, logo temos que:

$$\alpha(n) - \alpha(2) < \alpha(n-1) \tag{4.6}$$

Temos que existe um único $\alpha(l) \in \Delta(R, \rho, \varphi)$ tal que $\alpha(n) - \alpha(l) = \alpha(n-1)$, logo de 4.6 temos que $\alpha(l) < \alpha(2)$ o que é uma contradição. Suponha agora que $\alpha(n) - \alpha(i) = \alpha(n-i+1)$ para $i = 1, \cdots, k$, e vamos mostrar por indução que $\alpha(n) - \alpha(k+1) = \alpha(n-(k+1)+1)$. Suponha que $\alpha(n) - \alpha(k+1) \neq \alpha(n-(k+1)+1)$, então temos que:

$$\alpha(n) - \alpha(k+1) < \alpha(n-(k+1)+1) \tag{4.7}$$

Temos que existe um único $\alpha(s) \in \Delta(R, \rho, \varphi)$ tal que $\alpha(n) - \alpha(s) = \alpha(n-(k+1)+1)$, logo por 4.7 temos que $\alpha(s) < \alpha(k+1)$, isto é; $\alpha(s) \in \{\alpha(1), \alpha(2), \cdots, \alpha(k)\}$, o que é uma contradição pois $\alpha(n) - \alpha(i) = \alpha(n-i+1) > \alpha(n-(k+1)+1)$ para todo $i = 1, \cdots, k$. Logo, $\alpha(n) - \alpha(k+1) = \alpha(n-(k+1)+1)$.

(c) Seja s tal que $1 \leq s < n$, veja que:

$$C(\alpha(s)) = C^{\perp}(B, G), \text{ onde } G = \{b_i \mid \alpha(i) \leq \alpha(s)\} \text{ e}$$
$$E(\alpha(n-s)) = C(B, G), \text{ onde } G = \{b_i \mid \alpha(i) \leq \alpha(n-s)\}$$

Veja que $dim(E(\alpha(n-s))) = n - s$. Como $C(\alpha(s))$ é o código dual de $E(\alpha(s))$ segue que $dim(C(\alpha(s))) = n - dim(E(\alpha(s))) = n - s$. Assim, $dim(C(\alpha(s))) = dim(E(\alpha(n-s))) = n - s$.

(d) Para $\alpha(l_1), \alpha(l_2), \cdots, \alpha(l_t) \in \Delta(R, \rho, \varphi)$ defina:

$$h : N(\alpha(l_1)) \cup \cdots \cup N(\alpha(l_t)) \to M(\alpha(n) - \alpha(l_1)) \cup \cdots \cup M(\alpha(n) - \alpha(l_t))$$
$$\eta \longmapsto \alpha(n) - \eta$$

Seja $\eta \in N(\alpha(l_1) \cup \cdots \cup N(\alpha(l_t)))$, logo $\eta \in N(\alpha(l_j)$ para algum $j \in \{1, 2, \cdots, t\}$, logo pela definição da função g do item (a) temos que $\alpha(n) - \eta \in M(\alpha(n) - \alpha(l_j)) \subseteq M(\alpha(n) - \alpha(l_1)) \cup \cdots \cup M(\alpha(n) - \alpha(l_t))$, logo h está bem definida. Se $\alpha(n) - \eta_1 = \alpha(n) - \eta_2$ então $\eta_1 = \eta_2$ logo h é injetora. Seja γ um elemento do contradomínio de h, logo $\gamma \in M(\alpha(n) - \alpha(l_s))$ para algum $s \in \{1, 2, \cdots, t\}$, novamente pela definição da função g do item (a) temos que $\alpha(n) - \gamma \in N(\alpha(l_s))$ e $h(\alpha(n) - \gamma) = \gamma$, logo h é sobrejetora, e portanto uma bijeção. Assim,

$$\mu(\alpha(l_1), \cdots, \alpha(l_t)) = \sigma(\alpha(n) - \alpha(l_1), \cdots, \alpha(n) - \alpha(l_t)) = \sigma(\alpha(n - l_1 + 1), \cdots, \alpha(n - l_t + 1)) \tag{4.8}$$

Veja que $d_t(C(\alpha(s))) \geq min\{\mu(\alpha(i_1), \cdots, \alpha(i_t)) \mid \alpha(i_l) > \alpha(s)$ *para* $l = 1, \cdots, t$ *e* $\alpha(i_l) \neq \alpha(i_j)$ *para* $i \neq j\}$. Então $\alpha(i_l) \in \{\alpha(s+1), \cdots, \alpha(s+n-s)\}$ para $l = 1, \cdots, t$.(Veja que $t \leq k = n - s$).

E $d_t(E(\alpha(n-s))) \geq min\{\sigma(\alpha(j_1), \cdots, \alpha(j_t)) \mid \alpha(j_l) \leq \alpha(n-s)$ $\forall l = 1, \cdots, t$ *e* $\alpha(j_l) \neq \alpha(j_s)$ *para* $l \neq s\}$. Logo $\alpha(j_l) \in \{\alpha(1), \cdots, \alpha(n-s)\}$, para $l = 1, \cdots, t$. Sejam

$$A := \{(\alpha(s+i_1), \cdots, \alpha(s+i_t)) \mid i_l \in \{1, 2, \cdots, n-s\} \text{ e } i_s \neq i_k \text{ para } s \neq k\} \text{ e}$$
$$B := \{(\alpha(j_1), \cdots, \alpha(j_t)) \mid j_l \in \{1, 2, \cdots, n-s\} \text{ e } j_s \neq j_k \text{ para } s \neq k\}.$$

Definindo

$$\psi : A \longrightarrow B$$
$$(\alpha(s+i_1), \cdots, \alpha(s+i_t)) \mapsto (\alpha(n-(s+i_1)+1), \cdots, \alpha(n-(s+i_t)+1)).$$

Para cada $s+i_l$ com $i_l \in \{1, 2, \cdots, n-s\}$ temos que $s+1 \leq s+i_l \leq n$, logo $1 \leq n-(s+i_t)+1 \leq n-s$ e assim ψ está bem definida. Veja que se $\alpha(n-(s+i_1)+1), \cdots, \alpha(n-(s+i_t)+1)) = \alpha(n-(s+i_1')+1), \cdots, \alpha(n-(s+i_t')+1))$ então $(i_1, \cdots, i_t) = (i_1', \cdots, i_t')$, assim ψ é injetora. Como $\sharp(A) = \sharp(B)$ segue que ψ é sobrejetora, e logo é uma bijeção. Por 4.8 e pela construção de ψ temos que:

$$min\{\mu(\alpha(i_1), \cdots, \alpha(i_t)) \mid \alpha(i_l) > \alpha(s) \text{ para } l = 1, \cdots, t \text{ e } \alpha(i_l) \neq \alpha(i_j) \text{ para } i \neq j\} = min\{\sigma(\alpha(j_1), \cdots, \alpha(j_t)) \mid \alpha(j_l) \leq \alpha(n-s)\ \forall l = 1, \cdots, t \text{ e } \alpha(j_l) \neq \alpha(j_s) \text{ para } l \neq s\}.$$

(e) Temos que:

$$\tilde{E}(\delta) = C(B, G_1), \text{ onde } G_1 = \{b_i \mid \sigma(\alpha(i)) \geq \delta\} \text{ e}$$
$$\tilde{C}(\delta) = C^{\perp}(B, G_2), \text{ onde } G_2 = \{b_i \mid \mu(\alpha(i)) < \delta\}$$

Suponha que $dim(\tilde{E}(\delta)) = k$, logo existem $\alpha(i_1), \cdots, \alpha(i_k) \in \Delta(R, \rho, \varphi)$ tais que $\sigma(\alpha(i_l)) \geq \delta$ para $l = 1, \cdots, k$. E ainda, $\sigma(\alpha(i_l)) < \delta$ para $l \notin \{1, \cdots, k\}$. Como para cada $\alpha(s)$ existe um único $\alpha(l)$ tal que $\alpha(n) - \alpha(l) = \alpha(s)$ e $\mu(\alpha(l)) = \sigma(\alpha(n) - \alpha(l))$, existe uma bijeção entre os conjuntos $\{\mu(\alpha(l)) \mid l = 1, \cdots, n\}$ e $\{\sigma(\alpha(j)) \mid j = 1, \cdots, n\}$. Assim, existem $\alpha(j_1), \alpha(j_2), \cdots, \alpha(j_k) \in \Delta(R, \rho, \varphi)$ tais que $\mu(\alpha(j_l)) \geq \delta$ para $l = 1, \cdots, k$. E ainda, $\mu(\alpha(j_l)) < \delta$ para $l \notin \{1, 2, \cdots, k\}$. Assim, $dim(C(B, G_2)) = n-k$, logo $dim(C^{\perp}(B, G_2)) = n-n+k = k$.

(f)Temos que

$$d_t(\tilde{E}(\delta)) \geq min\{\sigma(\alpha(i_1), \cdots, \alpha(i_t)) \mid \sigma(\alpha(i_s)) \geq \delta \text{ para } s = 1, \cdots, t \text{ e } \alpha(i_j) \neq \alpha(i_s) \text{ para } j \neq s\}$$
e
$$d_t(\tilde{(C)}(\delta)) \geq min\{\mu(\alpha(j_1), \cdots, \alpha(j_t)) \mid \mu(\alpha(j_l)) \geq \delta \text{ para } l = 1, \cdots, t \text{ e } \alpha(j_l) \neq \alpha(j_s) \text{ para } l \neq s\}$$

Por 4.8, existe uma bijeção entre

$$\{\sigma(\alpha(i_1), \cdots, \alpha(i_t)) \mid \alpha(i_l) \in \Delta(R, \rho, \varphi)\ l = 1, \cdots, t\} \text{ e}$$
$$\{\mu(\alpha(j_1), \cdots, \alpha(j_t)) \mid \alpha(j_l) \in \Delta(R, \rho, \varphi)\ l = 1, \cdots, t\}$$

Assim, segue o resultado. ■

4.2 Exemplos

Nesta seção usaremos a notação $\langle \cdots \rangle$ com dois sentidos. Primeiramente, dados $F_1, \cdots, F_S \in \mathbb{F}_q[X_1, \cdots, X_m]$ denotamos por $\langle F_1, \cdots, F_s \rangle$ o ideal gerado pelos polinômios $F_1. \cdots, F_s$. Em segundo lugar, dados elementos $w_1, \cdots, w_m \in \mathbb{N}_0^r$ denotamos por $\langle w_1, \cdots, w_m \rangle$ o semigrupo gerado por $w_1, \cdots, w_m$.

Exemplo 4.2.1 *Considere o anel $R := \mathbb{F}_9[X, Y]/I$ onde I é o ideal gerado pelo polinômio hermitiano $X^4 - Y^3 - Y$. Sejam $w(X) = 3, w(Y) = 4 \in \mathbb{N}_0$, e considere a ordem usual (e única) $\prec_{\mathbb{N}_0}$ sobre $\mathbb{N}_0$, e ainda considere $\prec_{\mathcal{M}}$ a ordem grau-lexicográfica sobre $\mathcal{M}(X, Y)$ com $X \prec_{\mathcal{M}} Y$. A ordem generalizada grau com pesos resultante $\prec_w$ nos fornece a seguinte pegada para I:*

$$\Delta_{\prec_w}(I) = \{X^{\alpha} Y^{\beta} \mid 0 \leq \alpha,\ 0 \leq \beta < 3\}.$$

Agora, é fácil ver as condições do teorema 4.1.9 são satisfeitas com a base de Gröbner $\mathcal{G} = \{X^4 - Y^3 - Y\}$. Assim, como

$$\mathcal{G}' = \{X^4 - Y^3 - Y, X^9 - X\}$$

é uma base de Gröbner para I_9*, temos que* $\sharp\mathbb{V}_{\mathbb{F}_9}(I_9) = 27$*, onde* $I_9 = \{X^4 - Y^3 - Y, X^9 - X, Y^9 - Y\}$*. Logo podemos escrever* $\mathbb{V}_{\mathbb{F}_9}(I_9) = \{P_1, \cdots, P_{27}\}$ *e definir* $\varphi : R \to \mathbb{F}_9^{27}$ *por* $\varphi(F + I) = (F(P_1), \cdots, F(P_{27}))$*.*

$$\Delta_{\prec_w}(I_9) = \{X^\alpha Y^\beta \mid 0 \leq \alpha \leq 8,\ 0 \leq \beta \leq 2\}$$

Logo, as hipótese da proposição 4.1.16 são satisfeitas e veja que:

$$\Delta(R, \rho, \varphi) = \{0, 3, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 28, 29, 32\}.$$

Vamos ver outro exemplo:

Exemplo 4.2.2 *Seja* $I := \langle X^5 + Y^4 + Y, Y^5 + Z^4 + Z\rangle \subseteq \mathbb{F}_{16}[X, Y, Z]$*. Definimos a ordem generalizada com pesos* $\prec_w$ *sobre* $\mathcal{M}(X, Y, Z)$ *a seguir. Considere os pesos* $w(X) = 16$*,* $w(Y) = 20$*,* $w(Z) = 25 \in \mathbb{N}_0$*. Seja* $\prec_{\mathbb{N}_0}$ *a ordem monomial usual(e única) sobre* $\mathbb{N}_0$ *e seja* $\prec_M$ *a ordem lexicográfica sobre* $\mathcal{M}(X, Y, Z)$ *dada por* $X \prec_M Y \prec_M Z$*. Com relação a ordem resultante* $\prec_w$ *temos que* $\{X^5 + Y^4 + Y, Y^5 + Z^4 + Z\}$ *é uma base de Gröbner e por verificação observamos que as condições do teorema 4.1.9 são satisfeitas. Pelo teorema 4.1.9 obtemos portanto uma função peso:*

$$\rho : R := \mathbb{F}_{16}[X, Y, Z]/I \to \langle 16, 20, 25\rangle \cup \{-\infty\}.$$

Temos também que o conjunto $\{X^5+Y^4+Y, Y^5+Z^4+Z, X^{16}+X, Y^{16}+Y, Z^{16}+Z\}$ *é uma base de Gröbner para* I_{16} *com relação a* $\prec_w$ *e portanto* $\sharp(\mathbb{V}_{\mathbb{F}_{16}}(I_{16})) = \sharp(\Delta_{\prec_w}(I_{16})) = 256$*. Seja* φ *a aplicação de avaliação* $\varphi : R \to \mathbb{F}_{16}^{256}$ *dada por* $\varphi(f) = (f(P_1), f(P_2), \cdots, f(P_{256}))$*. Como* $\Delta_{\prec_w}(I_{16}) = \{X^a Y^b Z^c \mid 0 \leq a < 16,\ 0 \leq b < 4,\ 0 \leq c < 4\}$ *a pegada de* I_{16} *tem o formato de uma caixa, e portanto pela proposição 4.1.16 que a dimensão de* $\tilde{C}(\delta)$ *é igual a dimensão de* $\tilde{E}(\delta)$ *para todo* $\delta = 1, 2, \cdots, 256$*.*

Apenas para ilustração, temos que:

$$\Delta(R, \rho, \varphi) = \{0, 16, 20, 25, 32, 36, 40, 41, 45, 48, 50, 52, 56, 57, 60, 61, 64, 65, 66, 68, 70, 72, 73, 75, 76, 77, 80, 81, 82, 84, 85, 86, 88, 89, 90, 91, 92, 93, 95, 96, 97, 98, 100, 101, 102, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 120, 121, 122, 123, \cdots, 254, 255, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 273, 274, 275, 277, 278, 279, 280, 282, 283, 284, 285, 286, 287, 289, 290, 291, 293, 294, 295, 298, 299, 300, 302, 303, 305, 307, 309, 310, 311, 314, 315, 318, 319, 323, 325, 327, 330, 334, 335, 339, 343, 350, 355, 359, 375\}$$

Exemplo 4.2.3 *Considere* $I := \langle X^2 + YZ^2 - Y^2Z - X, U^2 - Z^3 + X^2 - Y^2Z + Y^3 + U\rangle \subseteq \mathbb{F}_4[X, Y, Z, U]$ *e defina a ordem generalizada grau com pesos* $\prec_w$ *sobre* $\mathcal{M}(X, Y, Z, U)$ *como a seguir. Considere os pesos* $w(X) = (2, 1), w(Y) = (0, 2), w(Z) = (2, 0), w(U) = (3, 0) \in \mathbb{N}_0^2$ *e seja* $\prec_{\mathbb{N}_0^2}$ *a ordem monomial grau-lexicográfica, com* $(0, 1) \prec_{\mathbb{N}_0^r} (1, 0)$*. Por último, seja* $\prec_{\mathcal{M}}$ *a ordem lexicográfica com* $Z \prec_{\mathcal{M}} U \prec_{\mathcal{M}} Y \prec_{\mathcal{M}} X$*. Veja que o monômio líder de* $X^2 + YZ^2 - Y^2Z - X$ *é* X^2*, pois:*

$$w(X^2) = w(YZ^2) = (4, 2),\ w(Y^2Z) = (2, 4),\ w(X) = (2, 1)$$

e $YZ^2 \prec_{\mathcal{M}} X^2$*. O monômio líder de* $U^2 - Z^3 + X^2 - Y^2Z + Y^3 + U$ *é* U^2*, pois*

$$w(U^2) = w(Z^3) = (6,0),\ w(X^2) = (4,2),\ w(Y^2Z) = (2,4),$$
$$w(Y^3) = (0,6),\ w(U) = (3,0)$$

e $Z^3 \prec_{\mathcal{M}} U^2$.
Como X^2 *e* U^2 *são relativamente primos, por um resultado da teoria das bases de Gröbner temos que* $G = \{X^2 + YZ^2 - Y^2Z - X,\ U^2 - Z^3 + X^2 - Y^2Z + Y^3 + U\}$ *é uma base de Gröbner para* I. *É fácil ver que as condições do teorema 4.1.9 são satisfeitas, e logo obtemos a função peso*

$$\rho : R := \mathbb{F}_4[X,Y,Z,U]/I \to \langle (2,1),(0,2),(2,0),(3,0)\rangle \cup \{-\infty\}$$

Usando o algoritmo de Buchberger podemos motrar que

$$\mathcal{G}' = \{X^2 + YZ^2 - Y^2Z - X,\ U^2 - Z^3 + X^2 - Y^2Z + Y^3 + U,\ X^4 - X, Y^4 - Y, Z^4 - Z, U^2 - U\}$$

é uma base de Gröbner para I_4, *logo*

$$\Delta_{\prec_w}(I_4) = \{X^\alpha Y^\beta Z^\gamma U^\delta \mid \alpha,\delta < 2 \text{ e } \beta,\gamma < 4\}$$

A pegada de I_4 *tem* 64 *elementos, cujos pesos são:*

$$\Delta_{\prec_w}(I_4) = \{(0,0),(0,2),(0,4),(0,6),(2,0),(2,1),(2,2),(2,3),(2,4),$$
$$(2,5),(2,6),(2,7),(3,0),(3,2),(3,4),(3,6),(4,0),(4,1),(4,2),(4,3),(4,4),(4,5),(4,6),(4,7),$$
$$(5,0),(5,1),(5,2),(5,3),(5,4),(5,5),(5,6),(5,7),(6,0),(6,1),(6,2),(6,3),(6,4),(6,5),(6,6),$$
$$(6,7),(7,0),(7,1),(7,2),(7,3),(7,4),(7,5),(7,6),(7,7),(8,1),(8,3),(8,5),(8,7),(9,0),(9,1),$$
$$(9,2),(9,3),(9,4),(9,5),(9,6),(9,7),(11,1),(11,3),(11,5),(11,7)\}$$

Podemos representar graficamente os pesos dos elementos de $\Delta_{\prec_w}(I_4)$ *como sendo os pontos pretos no gráfico abaixo:*

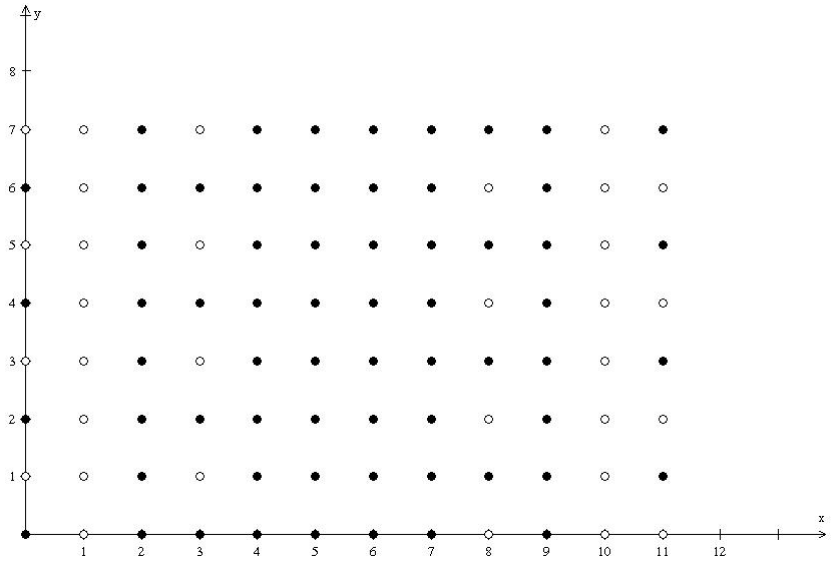

Figura 4.2: Os pesos dos elementos de $\Delta_{\prec_w}(I_4)$

Temos que $\Gamma = \langle (2,1),(0,2),(2,0),(3,0)\rangle$, *agora veja que as lacunas de* Γ *são os pontos do conjunto* L *definido como:*

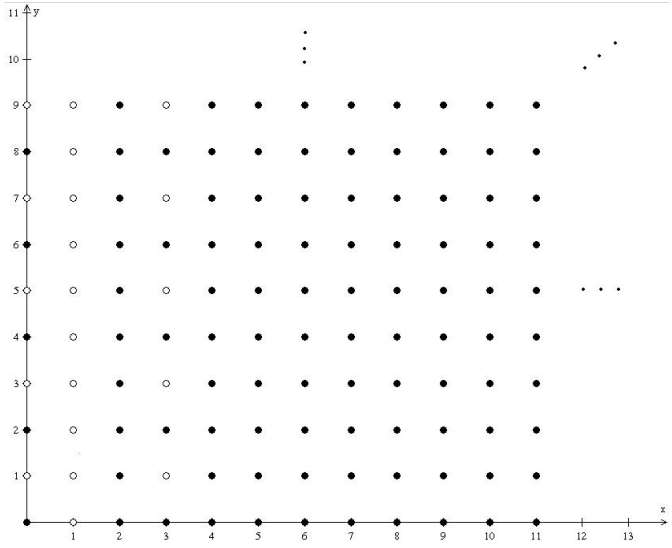

Figura 4.3: Os elementos de Γ

$$L := \{(a,b) \in \mathbb{N}_0^2 \mid a = 1\} \cup \{(a,b) \in \mathbb{N}_0^2 \mid a = 0 \text{ e } b = 2k+1, \text{ com } k \in \mathbb{N}_0\}$$
$$\cup \{(a,b) \in \mathbb{N}_0^2 \mid a = 3 \text{ e } b = 2k+1, \text{ com } k \in \mathbb{N}_0\}$$

podemos demonstrar que de fato L é o conjunto de todas as lacunas de Γ. Assim, podemos representar graficamente os pontos de Γ como sendo os pontos pretos no gráfico da figura 4.3.

Exemplo 4.2.4 *Seja $I := \langle X^5 + Y^4 + Y, Y^5 + Z^4 + Z, Z^5 + U^4 + U^2 \rangle \subseteq \mathbb{F}_{16}[X,Y,Z,U]$. Definimos a ordem generalizada com pesos $\prec_w$ sobre $\mathcal{M}(X,Y,Z,U)$ a seguir. Considere os pesos $w(X) = 64,\ w(Y) = 80, w(Z) = 100,\ w(U) = 125 \in \mathbb{N}_0$. Seja $\prec_{\mathbb{N}_0}$ a ordem monomial usual(e única) sobre $\mathbb{N}_0$ e seja $\prec_{\mathcal{M}}$ a ordem lexicográfica sobre $\mathcal{M}(X,Y,Z,U)$ dada por $X \prec_{\mathcal{M}} Y \prec_{\mathcal{M}} Z \prec_{\mathcal{M}} U$. As condições do teorema 4.1.9 são sastifeitas com a base de Gröbner $\{X^5 + Y^4 + Y, Y^5 + Z^4 + Z, Z^5 + U^4 + U^2\}$. Portanto temos uma função peso:*

$$\rho : R := \mathbb{F}_{16}[X,Y,Z,U]/I \to \langle 64, 80, 100, 125 \rangle \cup \{-\infty\}.$$

De acordo com o método de Andersen-Geil, deveríamos agora encontrar a pegada de I_{16}. Pelo algoritmo de Buchberger encontramos uma base reduzida de Gröbner com 21 *polinômios, listamos a seguir apenas os monômios líderes:*

$$\{Y^4, Z^4, U^4, X^{10}Y^2Z^2, X^5Y^2ZU^2, X^{10}ZU^2, X^5Y^2Z^3, X^{10}Z^3, X^{10}Z^3, X^{10}Y^3, X^{15}, XY^3Z^3U^2,$$
$$X^{11}U^2, X^6Z^2U^2, X^6Y^3Z^2, X^{11}Y, X^{11}Z, X^6YZU^2, X^6YZ^3, X^{10}Y^2U^2, X^5YZ^2U^2\}$$

Pela definição de base de Gröbner, a pegada de I_{16} consiste de todos os monômios que não são divisíveis por nenhum dos 21 *monômios acima. A pegada é encontrada como sendo de tamanho $n = 512$ e portanto temos um homomorfismo $\varphi : R \to \mathbb{F}_{16}^{512}$ para a construção de códigos. É claro que a pegada de I_q não tem o formato de uma caixa.*

Referências Bibliográficas

[1] H.E. Andersen and O. Geil, Evaluation codes from order domain theory, *Finite Fields and Their Applications*, (2008), pp. 92-123.

[2] D.Cox, J.Little, D.O'Shea; Ideals, Varieties and Algorithms; second ed; Springer; Berlim, 1997.

[3] O.Geil, R.Pellikan, On the structure of order domains; Finite Fields Appl. 8(2002) 369-396.

[4] T.Hoholdt, J.van lint, R.Pellikan; Algebraic geometry codes, in: V.S.Pless, W.C.Huffman (Eds.); Handbook of Coding Theory, vol 1, Elsevier, Amsterdan, 1998, pp.871-961(chapter 10).

[5] H.Stichtenoth, Algebraic Function Fields and Codes, second ed., Springer; Istambul, 2008.

[6] O. Geil, Evaluation codes from an affine variety code perspective, Advances In Algebraic Geometry Codes, E. Martinez-Moro, C.Munuera, D. Ruano, eds., World Scientific Publishing Co. Pte. Ltd., pp.153?180, 2008.

[7] T.Shibuya, K.Sakaniwa, A dual of well-behaving type designed minimum distance, IEICE Trans. Fund. E84-A(2001)647-652.

[8] A.I. Barbero, C.Munuera, The weight hierarchy of hermitian codes, SIAM J. Discrete Math. 13(2000) 79-104.

[9] P.Heijnen, R.Pellikan, Generalized Hamming weights of q-ary Reed-Muller codes, IEEE Trans. Inform. Theory 44(1998) 181-196.

[10] O.Geil, C.Thommesen, On the Feng-Rao bound for generalized Hamming weights, in: M.Fossorier, H.Imai, S.Lin, A.Poli(Eds.), Proc.AAECC-16, in: Lecture Notes in Comput. Sci., vol 3857, Springer, Berlim, 2006 pp.295-306.

[11] Hefez, A., Villela, M.L.T., Códigos Corretores de Erros, Série de Computação e Matemática, 2002.

[12] C.E. Shannon, A mathematical theory of communication, Bell System Technical Journal, vol 27, 1948.